LAUREA AMMATTIKORKEAKOULU Uuden edellä

Käyttöoikeushallintaprosessin kehittäminen Vantaan kaupungin organisaatiossa: tapaustutkimus

Guday, Tewodros

2012 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Käyttöoikeushallintaprosessin kehittäminen Vantaan kaupungin organisaatiossa: tapaustutkimus

Tewodros Guday
Tietojärjestelmäosaamisen koulutusohjelma ylempi AMK
Opinnäytetyö
Joulukuu, 2012

Sisällys

Tutkijan kiitokset

Aluksi haluaisin osoittaa suuret kiitokset ohjaajalleni Rauno Piriselle arvokkaista kommenteista ja kannustamisesta.

Haluaisin kiittää kaikkia tähän tutkielmaan kommenttinsa antaneita. Olen erittäin kiitollinen Tapio Huttuselle, että kaikesta kiireistä huolimatta löytyi aikaa ja mielenkiintoa jakaa näkemyksesi ja antaa arvokkaat kommenttisi. Tämä apu on ollut korvaamatonta. Inspiraatio aiheeseen nousi Vantaan tietohallinnon palvelukeskuksen käyttäjähallintatiiminvetäjän tehtävissä, minkä vuoksi suuri kiitos kuuluu tietohallintojohtajille Minna Ulvilalle ja Jonna Engblomille.

Suuri kiitos myös Pinja Lähteenmäelle, Tuula Mujeelle, Marjut Karrille, Jari Välilälle, jotka ovat aina auttaneet ja kannustaneet minua kaikin mahdollisin tavoin. Kiitos kuuluu myös haastattelut antaneille henkilöille.

Haluaan omistaa tämän tutkielman rakkaalle äidilleni (ATHNAFE GUDAY), joka iskosti sieluuni jo varhaisessa vaiheessa sen, miten arvokas asia koulutus on ihmiskunnalle.

Omistan tämän tutkielman arvokkaalle perheelleni, joka on tukenut minua ja ollut vierelläni koko tutkinnon ja tutkimusprosessin ajan. Erityisesti suuri kiitos kuuluu rakkaalle puolisolleni, joka tukenut minua ja auttanut tutkielman oikolukemisessa. (Outi, Leo ja Joel)

Espoossa, 18.12.2012

Laurea-ammattikorkeakoulu
Laure Leppävaara
Tietojärjestelmäosaamisen koulutusohjelma
Ylempi AMK

Tiivistelmä

Tewodors Guday

Käyttöoikeushallintaprosessin kehittäminen Vantaan kaupungin organisaatiossa: tapaustutkimus

Vuosi 2012 Sivumäärä 100

Tämän tutkimuksen kohde on selvittää nykyisen käyttäjätunnus- ja käyttöoikeushakuprosessin tuntemusta esimiesten keskuudessa Vantaan kaupungilla. Tarkoituksena on erityisesti tutkia sitä, minkälaisia käsityksiä esimiehillä on käyttöoikeuksien hausta alaisilleen. Työn aihealue on rajattu organisaation käyttäjätunnus- ja käyttöoikeushakuprosessin tuntemukseen, sekä sen puutteista johtuviin tietoturva-aukkoihin, sekä prosessin kehittämiseen.

Tutkimuksen lähtökohta on vuoden 2011 keväällä Vantaan kaupungin sisäisen tarkastuksen suorittama tarkastus merkittävimpien tietojärjestelmien käyttäjähallinnassa. Tarkastuksessa havaittiin, että esimiehillä ei välttämättä aina ole riittävää tietoa, siitä kuinka laajoja käyttöoikeuksia heidän alaisillaan on eri järjestelmiin. Samaan aikaan Vantaan kaupungilla oli vireillä käyttäjähallinnan (IDM) Identity Management kehittämishanke, jonka kohdealueena oli mm. keskitetty käyttäjähallintajärjestelmä ja kertakirjautumisratkaisu. Hankkeessa todettiin tarpeelliseksi muun muassa käyttäjähallinnan ja käyttöoikeuksienhallinnan sekä niihin liittyvien prosessien kehittäminen.

Tutkimuksen pääkysymys on: Miten käyttäjätunnuksien ja käyttöoikeuksien haku- ja käsittelyprosessi tunnetaan? Tutkimuksen osatavoite on todeta mitkä asiat ovat epäselviä ja mitä erityishaasteita on käyttäjätunnuksien- ja käyttöoikeuksien haku- ja käsittelyprosessissa.

Tutkimus toteutettiin tapaustutkimuksena (Case Study Research Analysis). Suunnittelutieteellistä tutkimusmetodologian käytön tavoitteena on luoda tietämystä ja suunnittelua käytännön toteutuksessa järjestelmää kehitettäessä (Design Science Research). Tutkimus tehtiin lähettämällä esimiehille tutkimuskysely ja haastattelemalla organisaation merkittävien järjestelmien pääkäyttäjiä eri toimialoilta. Lisäksi käytettiin käyttäjätunnuksia koskevaa, taustajärjestelmästä saatua tilastollista tietoa. Tutkimuskysely, haastattelut ja tilastoaineiston kokoaminen toteutettiin vuosien 2011 – 2012 aikana. Tietojärjestelmäkehittämiä tutkittaessa on käsitelty vaiheistus- ja elinkaarimalleja tietojärjestelmäkehitykselle ja – toteutukselle. Tutkimuksessa analysointiyksikkö oli näyttö esimiesten käyttäjähallintaprosessin tuntemuksesta.

Tutkimustulos osoitti, että käyttöoikeuksin merkitys ja sisältö tulisi kuvata aiempaa paremmin ja ymmärrettävämmin esimiehille. Esimiesten on tiedettävä mikä on heidän alaisilleen hakemiensa käyttöoikeuksien laajuus, niiden mahdollistamat toiminnat ja soveltuvuus suhteessa alaisen työtehtäviin sekä kuka on yhdyshenkilö käyttöoikeuksien asioissa. Esimiehen tietämättömyys alaisten käyttöoikeuksia arvioitaessa ja haettaessa saattaa vaarantaa organisaation tietoturvaa sekä hidastaa käyttöoikeuksien haku- ja käsittelyprosessia.

Kehitystoimenpiteenä tutkimuksesta saatujen tulosten pohjalta on esitetty organisaatiolle käyttöoikeushakemusprosessin kehittämistä ja uusia tapoja, joilla voidaan esittää käyttöoikeuksien sisältö esimiehelle ymmärrettävällä tavalla. Tutkimuksella on merkitystä siten, että saatujen tuloksia hyödyntämällä voidaan parantaa käyttäjätunnus- ja käyttöoikeushakuprosessia sekä kiinnittää huomiota esimiesten ymmärryksen syventämiseen käyttöoikeuksien sisällöstä ja laajuudesta. Tutkimus parantaa organisaation tietoturva huomattavasti.

Asiasanat: Käyttöoikeus, Rooli, IAM, IDM, Vaaralliset työyhdistelmät, tietojärjestelmät

Laurea University of Applied Sciences

Laurea Leppävaara
Master Degree in Information Systems

Tewodros Guday

Identity and Access Management process development in city of Vantaa: Case Study

Year 2012 Pages 100

Abstract

The main task of this study is to find out the understanding of the current Identity and Access Management (IAM) process among the superiors in the City of Vantaa. Furthermore, it is also researcher's intention to survey especially what adequate understanding the superiors have of the user management system when processing and proposing information system user rights for their subordinates. The subject matter of the work is limited to the management level understanding of the user management system of the organization.

The starting point for the study was the inspection the City of Vantaa internal audit unit performed in the spring 2011. Internal audit implemented a user rights inspection of the most significant information systems. In this inspection the result was that in some cases superiors do not necessarily have enough knowledge to evaluate what levels of user rights are adequate for their subordinates to do their job tasks. As a result of the study research, the developing project of user management system presented itself as a necessary step towards to have a significantly easier understanding of the content of the user role(s) and sustainable Identity and Access Management process.

The study carried out as a Case Study Research Analysis and Design Science Research study methodology while developing an Information System. The study was conducted by sending a research questions to the superiors, by interviewing the application owners of the significant information systems of the organization from different organization branches and furthermore, used statistical information about creation and deletion of user id from background system. The Case Study research and interviews, was carried out and statistics material collected during 2011 –2012. While studying developing Information System, the phase and life cycle model of information system was studied and implemented. The understanding of user management process is used as a unit of analysis in the study.

The research result shows that user roles have not been described in a sufficient way to the superiors. The superiors are not able to know what the scope of the user roles is, what operations can be done with them, what and how appropriate user role is needs to have to their subordinate, and who is the right contact person for the an individual user role. This creates a potential information security risk for the organization and slows down the process of Access Management and processing requests of superiors.

Based on the results obtained in the research study, "user role profile" standard model is presented as a possible development action. The standard model offers a method to present the contents of user roles can in a way that is understandable to the superiors.

As further study, it is suggested improving information security, requirement of the combinations of the IT roles and business roles. The identification of separations of risky work or task combinations and how to do the evaluation description of their risks has to be studied. The research plays a role in the fact that the obtained results can improve the Identity and Access Management process, as well as the deep understanding of managers to pay attention in the content and scope of user roles. It will also improve the organization security.

Keywords: User role, IAM, IDM, Segregation Duties SoD, Information Systems

1 Johdanto

Tietojärjestelmien tullessa yhä monimutkaisemmiksi muun muassa niiden käytön hallittavuus, käytettävyys, tietoturva, lainsäädäntö sekä viranomaisten asettamat vaatimukset ja suositukset tuovat ison haasteen eri organisaatioiden tietohallintoyksiköille. Tämän tutkimuksen kohde, käyttöoikeuksien hallinta on eräs kriittinen osa-alue, joka vaati tietohallinnolta jatkuvaa seurantaa, arviointia ja kehittämistä.

Toimintaympäristön muutokset (esimerkiksi uudet käyttäjäryhmät, uudet verkkopalvelut ja tiedonjakotavat, uudet käytettävissä olevat palvelut ja tekniikat esim. verkko- ja pilvipalvelut, mobiilipäätelaitteet) ja järjestelmien käyttäjien odotukset luovat tietohallinnolle paineen kehittää ja arvioida perinteisiä, pääsääntöisesti järjestelmäkohtaisia käyttöoikeushallinnan lähestymis- ja toteutustapoja. Nämä prosessit ovat usein hajautettuja, päällekkäisiä, epäselviä, epäyhdenmukaisia ja riskialttiita.

Vuoden 2011 keväällä Vantaan sisäinen tarkastus suoritti tarkastuksen Vantaan kaupungin merkittävimpien tietojärjestelmien käyttäjähallinnasta. Sisäisen tarkastuskertomuksen mukaan ”Esimiehet eivät aina voi tietää, mitä ja kuinka laajoja käyttöoikeuksia eri järjestelmiin heidän alaisillaan on. Tilanne korostuu yksiköissä, joissa henkilöstön vaihtuvuus on suurta. Esimiehet kuitenkin päättävät ja ovat vastuussa alaistensa käyttöoikeuksista ja siksi heidän on syytä valvoa niitä säännöllisesti”. (Vantaan sisäinen tarkastuskertomus 2011.)

Sisäinen tarkastuksen toimenpide-ehdotus on tehty järjestelmien pääkäyttäjien antamien haastatteluiden perusteella. Vaikka tehty haastattelututkimus oli otoskooltaan ja laajuudeltaan suppea, jäi haastattelun toimenpide- ehdotukset kaivelemaan mieltä. Päällimmäiseksi kysymykseksi nousi, mistä johtuu esimiehien tietämättömyys käyttäjätunnus- ja käyttöoikeushakuprosessin sekä käyttöoikeuksien laajuudesta ja kuinka sitä voitaisiin parantaa?

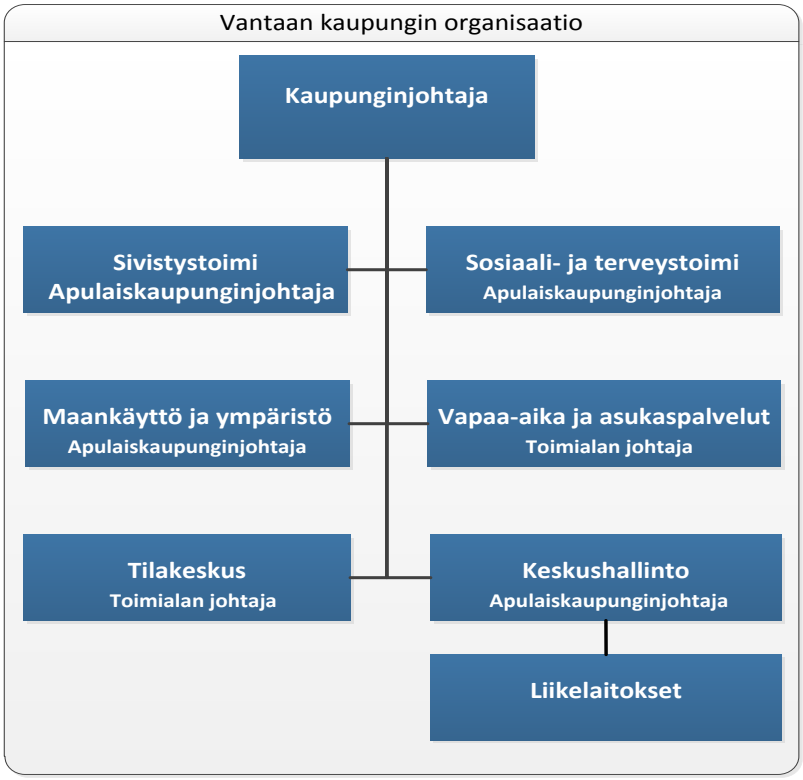
Tämän tutkimuksen tavoitteena on selvittää, miten Vantaan kaupungin esimiehet ymmärtävät käyttäjätunnus- ja käyttöoikeushakuprosessin sekä käyttöoikeuksien sisällön.

Osana tutkimustyötä toteutettiin nykyisiä käyttäjähallinta- ja käyttöoikeuspyyntökäytäntöjä koskevalla kyselyllä Vantaan kaupungin esimiehille sekä haastattelemalla kolmea pääkäyttäjää. Tutkimuskysely toteutettiin käyttöliittymältään www-selainpohjaisella Webropol-ohjelmalla. Tutkimustulosten perusteella on esitetty käyttöoikeushakuprosessiin ja sen sisältöön liittyviä kehitysideoita ja malli, jota voitaisiin soveltaa Vantaan käyttäjä- ja käyttöoikeushallinnan kehittämisessä. Käyttöoikeusprofiilin kuvaamismallin avulla on tarkoitus saavuttaa enemmän hyötyä käyttöoikeushallintaprosessista.

2 Organisaation ja tutkimuksen tausta

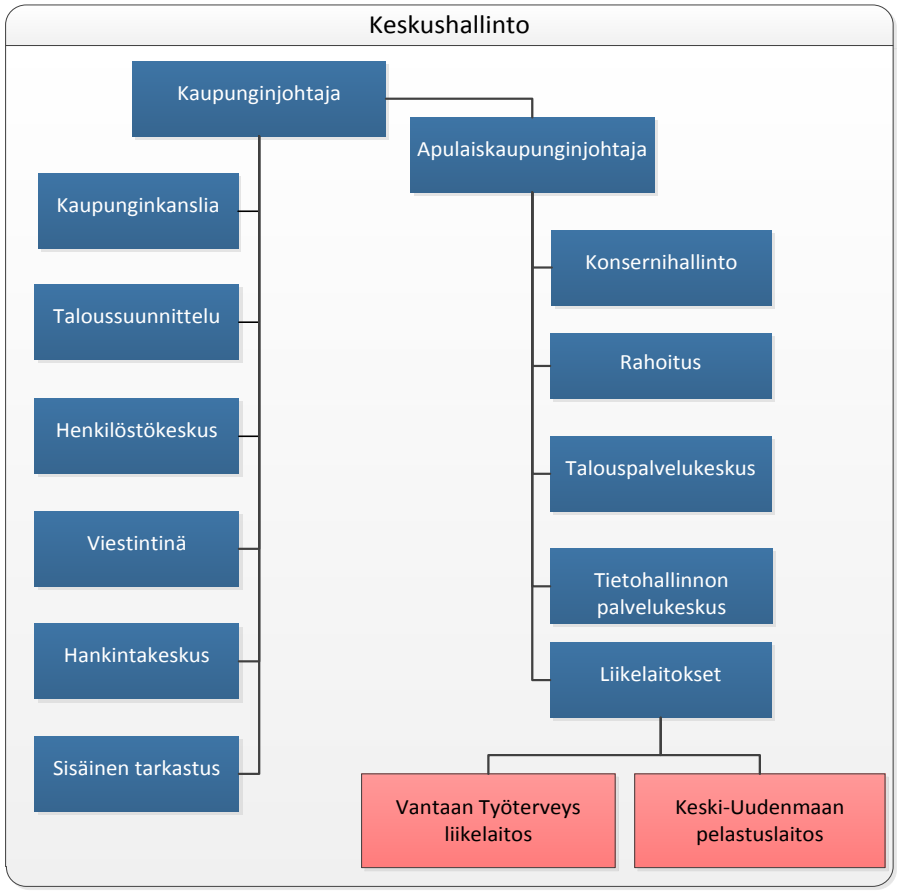
2.1 Vantaan kaupungin organisaatio

Vantaan kaupunki on yksi Helsingin metropolialueen kaupungeista. Vantaalla on asukkaita noin 200 000. Vantaan kaupungissa työskentelee lähes 12 000 työntekijää ja organisaatiota johtaa kaupunginjohtaja. Kaupunginjohtajan alaisuudessa toimivat neljä apulaiskaupunginjohtajaa ja kaksi toimialajohtajaa. Syksyllä 2012 organisaatio muodostui kuudesta toimialasta: keskushallinto, maankäyttö ja ympäristö, sivistystoimi, sosiaali- ja terveydenhuolto, tilakeskus sekä vapaa-aika ja asukaspalvelut. Suurin osa organisaation toimialoista jakautuu tulosalueisiin ja tulosyksikköihin. Tämän kehittämistutkimuksen aikana tilakeskuksen toimialalta eriytettiin siivous- ja ateriapalvelujen toiminnat yhdeksi osakeyhtiöksi Tilapalvelut Oy (tämä muutos ei ilmene kaaviokuvassa 1). Vantaan kaupungin palveluksessa työskentelee noin 900 henkilöä esimiestehtävissä.



Kuvio 1: Vantaan kaupungin organisaatio 1.1.2011

Tietohallinnon palvelukeskus sijoittuu kaupungin keskushallinnon organisaatiossa yhdeksi tulosalueeksi (kuvio 2). Tulosalue jakautuu neljään tulosyksikköön: IT-projektit, teknologia, asiakkaat ja sovellukset sekä infrastruktuuri. Nykyinen tietohallinnon palvelukeskus on perustettu vuonna 2007. Tällä hetkellä palvelukeskuksessa työskentelee noin 50 työntekijää.



Kuvio 2: Keskushallinnon organisaatio (v. 2011)

Tietohallinnon palvelukeskus vastaa Vantaan kaupunkikonsernin palvelutuotannossa tarvittavasta ICT-teknologiasta ja -palveluista. Toimialat vastaavat järjestelmäratkaisuiden sisällöistä. Heillä on myös tietojärjestelmiensä pääkäyttäjä- ja henkilötietolain mukainen rekisterinpitäjävastuu. Tietohallinnon palvelukeskuksen ydintehtäviä ovat: 1) osaava ja tehokas tietojärjestelmien, -teknologioiden ja -palveluiden hankinta, tuotanto ja ohjaus; 2) kaupunkitasoisten tietojärjestelmien ja -palveluiden yhtenäisyyden varmistaminen (kaupunkitasoiset arkkitehtuuriratkaisut); 3) aktiivinen, asiantunteva ja strateginen kumppani konsernissa sekä; 4) toimialoja palvelevien ICT-ratkaisujen omistajuus.

Tietohallinnon palvelukeskus vastaa suuresta osasta kaupungin yhteisten ja osin toimialakohtaistenkin järjestelmien käyttäjätunnuksien ja käyttöoikeuksien hallintaprosesseista. Lisäksi se suunnittelee pääkäyttäjien kanssa yhteistyössä eri järjestelmien käyttöoikeuksien hakuprosessit sekä tuottaa sähköistä käyttäjätunnus- tai käyttöoikeushaku- ja -hyväksyntäpalvelua toimialoille itsepalveluna. (Vantaan kaupungin tietohallinnon ydintehtävät 2011.)

2.2 Tutkimuksen tausta

Vantaan kaupunki käynnisti vuonna 2010 käyttäjähallinnan (IDM) Identity Management kehittämishankkeen. Hankkeen käynnistäminen perustui käytännössä todettuun tarpeeseen kehittää ja yksinkertaistaa muun muassa käyttäjähallintaa ja käyttöoikeuksienhallintaa sekä niihin liittyviä prosesseja. Hankkeen tavoitteina oli keskitetty käyttäjähallintajärjestelmä ja kertakirjautumisratkaisu. Keväällä 2010 sisäinen tarkastus suoritti organisaation merkittävimpien tietojärjestelmien käyttäjähallinnan osalta sisäisen tarkastuksen. Tarkastusraportin tulos ja toimenhoide-ehdotukset antoivat tutkimuksen tekijälle impulssin selvittää, miksi esimiehillä ei välttämättä ole riittävästi tietoa eri järjestelmien käyttöoikeuksien sisällöstä ja niiden merkityksestä. Esimiehillä on kuitenkin vastuu alaistensa käyttöoikeuksista ja niiden laajuudesta suhteessa esimerkiksi alaisten työtehtäviin. Näiden tietämyspuutteiden selvittämiseksi ja käyttäjätunnushakuprosessin kehittämiseksi päädyttiin tutkimaan, kuinka tärkeänä Vantaan kaupungin esimiehet pitävät käyttäjätunnushakuprosessia ja käyttöoikeuksien sisältöä.

2.2.1 Aiheen valinta

Nykyaikaiset organisaatiot ovat ottaneet käyttöön monenlaisia tietojärjestelmiä ja ICT-infrastruktuurikomponentteja liiketoiminta strategiansa toteutuksen ja tavoitteiden saavuttamisen tueksi. Näihin tietojärjestelmiin on pääsy erilaisilla käyttäjäryhmillä esimerkiksi työntekijöillä, yhteistyökumppaneilla ja asiakkailla. ICT-infrastruktuurin monimutkaisuuden, tietojärjestelmien ja käyttäjien määrän kasvaessa, myös käyttäjäryhmien ja heille tarjottavien palveluiden monimuotoisuus lisääntyy. Tällöin perinteiset työkalut ja manuaalinen käyttäjätunnusten hallintaprosessi ovat osaltaan tietoturvariski, jonka toteutumisen seurauksena ääritapauksessa organisaatio voi menettää merkittäviä tietoja. Käyttäjähallinta- ja käyttöoikeusprosessien kehittämiseksi IT-alalla on tehty erilaisia tutkimuksia. Kuntaorganisaatioissa on ollut useita eritasoisia hankkeita ja aikeita keskitetyn käyttäjähallintajärjestelmä ja käyttövaltuushallinnan kehittämiseksi sekä kertakirjautumis-ratkaisun luomiseksi. Esimerkiksi Tampereen kaupunki haki vuonna 2007 kilpailuttamalla keskitettyä käyttäjähallintaratkaisua. Syksyllä 2012 Kuntaliitto käynnisti käyttövaltuushallinnan viitearkkitehtuurin luomiseen tähtäävän hankkeen osana kuntien yhteistä kokonaisarkkitehtuurityötä.

Vantaalla todettiin, että kokonaisvaltaisen keskitetyn käyttäjähallintaratkaisun toteuttamiseksi on tärkeää selvittää nykyinen tilanne ja arvioida kehittämistarpeita ja -kohteita yhteistyössä järjestelmien pääkäyttäjien ja esimiehien kanssa. Tämä selvitystyö antoi mahdollisuuden tutkia ja arvioida Vantaan kaupungin käyttäjätunnus- ja käyttöoikeushakuprosessien kehittämistä ja ratkaisuvaihtoehtoja.

2.2.2 Tutkimuksen tavoite

Tämän tutkimuksen tavoitteena on kerätä käyttökokemuksia, kehitysideoita sekä siten kehittää nykyistä käyttäjätunnus- ja käyttöoikeushallintaprosessia sekä kartoittaa erityisesti sitä, minkälaisia käsityksiä esimiehillä on käyttöoikeuksien hausta alaisilleen. Tutkimuksen tavoitteena on ollut myös selvittää, mitä on keskitetty käyttäjätunnus- ja käyttöoikeushakuprosessi, mitä haasteita siihen liittyy sekä millaisilla työvälineillä tai ratkaisumalleilla nämä haasteet voitaisiin voittaa. Tässä tutkimuksessa pyritään myös selvittämään millaisia keskitetyn käyttäjähallinnan- ja kertakirjautumisen ratkaisuja markkinoilla on tarjolla. Tässä tutkimuksessa rajataan ulkopuolelle käyttäjähallinta- ja kertakirjautumisjärjestelmäratkaisujen taloudellinen näkökulma: hankinta-, toteutus- ja käyttökulut sekä niillä mahdollisesti saavutettavat suorat ja välilliset säästöt. Tarkoituksena ei myöskään ole tarkastella organisaation yksittäisiä työntekijöitä, vaan käsitellä käyttäjäryhmiä yleisellä tasolla kokonaisuutena ja anonyymeinä.

2.2.3 Tutkimuskysymykset

Tämän tutkimuksen päätutkimuskysymys on seuraava: Miten organisaation käyttäjätunnus- ja käyttöoikeuksienhakuprosessi ja sen sisältö ymmärretään esimiesten keskuudessa? Tutkimuksen osatavoitteena on myös tarkastella sitä, miten tutkimuksen tulos analysoidaan eri ulottuvuuksilla seuraavilla kysymyksillä.

1. Mikä koetaan epäselväksi käyttäjätunnuksien- ja käyttöoikeuksienhaku- ja käsittelyprosessissa?
2. Onko jossain organisaation osassa erityisiä haasteita käyttäjätunnus- ja käyttöoikeushallintaprosessin suhteen?
3. Miten mahdollinen tiedon puute ja mahdolliset virheelliset käsitykset käyttäjätunnuksien ja käyttöoikeuksien hakuprosessista vaikuttavat organisaation toimintaan ja tietojärjestelmien käyttöön?

2.2.4 Tutkimuksen kohde ja rajaus

Lähes kaikki Vantaan noin 900:sta esimiestä rekrytoi uusia työntekijöitä, tekee työsopimuksia ja tässä yhteydessä hakee tai hyväksyy alaisilleen käyttäjätunnuksia ja käyttöoikeuksia eri tietojärjestelmiin (taulukko 1). Siksi tutkimuskyselyn lähettäminen esimiehille oli luonteva valinta. Kyselyyn vastanneiden valinta perustui heidän esimiesasemaansa. Heistä kyselyn kohdejoukkoon valittiin ne, jotka tekevät käyttäjätunnus- ja käyttöoikeuspyyntöjä omille alaisilleen organisaation käyttöoikeushakua varten käytössä olevasta järjestelmästä.

Toimiala	Työntekijöiden määrä	Esimiehien määrä	Kyselyn saaneet	Kyselyn vastanneet
Keski-Uudenmaan Pelastuslaitos	500	85	1	1
Keskushallinto	390	57	18	8
Maankäyttö ja Ympäristö	784	128	19	5
Sivistystoimi	5596	335	49	13
Sosiaali- ja terveydenhuolto	3192	177	58	26
Suun terveydenhuolto	320	17	1	1
Tilakeskus/ Tilapalvelut	1066	57	22	5
Vantaan Työterveys	71	5	1	0
Vapaa-aika ja Asukaspalvelut	914	57	13	5
Yhteensä	12833	918	182	64

Taulukko 1: Kaupungissa olevien esimiesten määrä toimialoittain

Esimiesten lisäksi tutkimuksen tekijä haastatteli Vantaan kaupungin organisaation kolmea merkittävimmin järjestelmän pääkäyttäjää. Nämä pääkäyttäjät edustivat sivistystoimen, sosiaali- ja terveystoimen ja keskushallinnon toimialoja. Haastateltavien henkilöiden valinnan perusteena oli heidän vastuullaan olevien järjestelmien merkittävyys ko. toimialan operatiivisen toiminnan kannalta. Lisäksi näiden valittujen toimialojen henkilöstömäärä on noin 75 % koko kaupungin henkilöstömäärästä ja työntekijöiden vaihtuvuus on suurin. Näiden merkittäväksi arvioitujen järjestelmien käyttäjien ja käyttöoikeuksien määrä on suuri. Haastatellut pääkäyttäjät ovat työskennelleet Vantaan kaupungin palveluksessa 20 – 30 vuotta ja pääkäyttäjätehtävissä 2- 8 vuotta. Alla on kuvattu pääkäyttäjien edustama toimiala, työkokemus Vantaa palveluksessa ja pääkäyttäjätehtävissä sekä heidän vastuullaan olevien järjestelmien käyttäjien ja käyttöoikeuksien määrä (taulukko 2).

Haastateltava	Pääkäyttäjän työkokemus		Pääkäyttäjän vastuulla oleva järjestelmä	
	Vantaan palveluksessa	Pääkäyttäjä tehtävissä	Järjestelmän käyttäjämäärä	Järjestelmän käyttöoikeuksien määrä
Pääkäyttäjä 1	Yli 20 V	Yli 3 v	3000	109
Pääkäyttäjä 2	30 V	8 v	603	51
Pääkäyttäjä 3	20 V	2 v ja 8 kk	947	1224

Taulukko 2: Haastateltavien pääkäyttäjien taustatiedot sekä järjestelmien käyttäjien ja käyttöoikeuksien määrä.

Tämä tutkimus on rajattu sitten, että tutkimuskohteena ovat esimiehet ja kolme pääkäyttäjää. Tutkimuksessa keskitytään seuraaviin aiheisiin: 1) Vantaan kaupungin käyttäjätunnus- ja käyttöoikeushakuprosessi; 2) käyttöoikeuskäsite ja käyttöoikeuksien laajuus; 3) vaaralliset työyhdistelmät sekä; 4) käyttäjähallintaprosesseja ja kertakirjautumisen toteuttamista tukevat ratkaisut.

3 Kehittämistutkimustyön teoreettinen tausta

Tässä luvussa tutustutaan kehittämistutkimustyön teoreettiseen tausta-aineistoon. Aineisto koostuu seuraavista aiheista: 1) käyttäjäidentiteettien ja käyttövaltuuksien hallintajärjestelmän (IAM) kokonaisratkaisu, käsitteet ja käyttäjähallinnan ydinosa-alueet; 2) käyttövaltuushallinnan hallintaprosessi, käyttäjäroolit, käyttövaltuutuksien määrittely, käyttövaltuuksien muutos-, myöntämis-, ja valvontaprosessit sekä käyttäjähallintaan ja käyttöoikeuksiin liittyvien prosessien tietosisältö; 3) käyttäjähallinnan prosessia tukevien ratkaisujen saatavuus; 4) lainsäädännön ja tietoturvan huomioonottaminen käyttäjähallinta- ja käyttöoikeusprosesseja kehitettäessä sekä; 5) järjestelmähankkeissa ja niihin liittyvien prosessien kehittämisessä huomioonotettavat mahdolliset riskit.

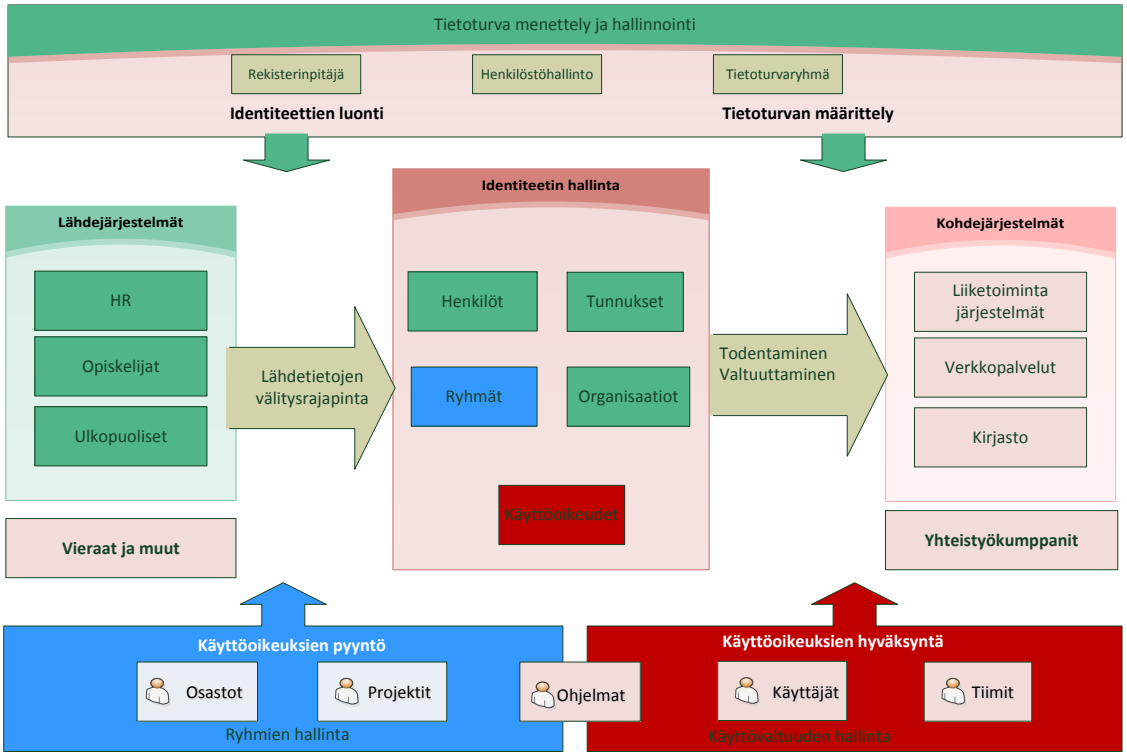
3.1 Käyttäjäidentiteettien ja käyttövaltuuksien hallintajärjestelmä (IAM)

Käyttäjäidentiteettien ja käyttövaltuuksien hallintajärjestelmä (IAM) Identity and Access Management muodostuu automaattisesta luvitusprosessista, keskitetystä käyttäjä- ja käyttövaltuushallinnan tietovarastosta, käyttövaltuustietojen provisioinnista ja raportointitoiminnosta (Kuvio 3). Käyttäjän identiteetti on muutakin kuin mitä käyttäjän sähköinen identiteetti on. Jatkossa käyttäjäidentiteetti- käsitteellä tarkoitetaan tässä tutkimuksessa ko. henkilön sähköistä tai digitaalista identiteettiä.

Järjestelmien pääsyhallinta- ja käyttövaltuushallintajärjestelmillä on tärkeä rooli organisaation liiketoimintatavoitteiden toteuttamisessa mm. tahallisten tai tahattomien väärinkäytösten estämisessä. IAM-järjestelmä yhdistää liiketoimintaprosesseja, tietoturvakäytäntöjä ja teknologiaa sekä auttaa organisaatioita hallitsemaan työntekijöidensä sähköisiä identiteettejä ja valvomaan pääsyä organisaation eri resursseihin. Rai, LLP, LLP, Bresz, Renshaw, Rozek & White (2007) vahvistavat IAM:n järjestelmien etujen olevan: nopea vasteaika, mahdollistaa helposti saatavat todisteet järjestelmän toiminnan teet, automatisoitujen työnkulkujen hyväksyntä ja viestintä, helpottaa suurten tietomäärien parempaa hallintaa, sekä kyky keskitetysti hallinnoida ja valvoa järjestelmiä. (Linares 2005, 9; Rai, LLP, LLP, Bresz, Renshaw, Rozek & White 2007, 11.)

Kasasen (2010) ja Jackson:n (2008) mukaan identiteetinhallinnalla tarkoitetaan käyttäjän sähköisen identiteetin ja siihen liitettyjen käyttövaltuuksien hallintaa, sekä tämän identiteetti- ja käyttövaltuustiedon välittämistä sitä tarvitseville tahoille. Hänen mukaansa identiteetinhallinnan perimmäisenä tarkoituksena on taata, että oikeilla käyttäjillä on pääsy oikeisiin resursseihin oikeaan aikaan mahdollisimman helposti ja tehokkaasti. Penn State Universty (2008) puolestaan kuvaa IAM:n käsitteitä ja prosesseja voidaan karkeasti jakaa kolmeen ryhmään: 1) Ihmiset ja suhteet; 2) identiteettien luominen ja ylläpito sekä; 3) Pääsy tietoihin ja sovelluksiin.

Shuey & Weidner (2008) määrittelevät sähköisen identiteetin ja käyttövaltuushallinnan (IAM) teknologiseen tai tekniseen ratkaisuun perustuvaksi hallinnolliseksi prosessiksi, joka varmistaa yksittäisten henkilöiden tai käyttäjien sähköisen identiteetin oikeellisuuden. (Kasanen 2010; Jackson 2007; Penn State Uinversty 2008; Shuey & Weidner 2008.)



Kuvio 3: Käyttäjäidentiteettien ja käyttövaltuuksien hallintajärjestelmä (IAM) malli (mukaillen Jackson 2007)

IAM-järjestelmä luo tiedon tai datan, sovellusten ja tietojärjestelmien omistajille mahdollisuuden hoitaa niiden käyttöoikeuksien myöntämisen joko keskitetysti tai vastuuta hajauttamalla kulloinkin kyseessä oleviin resursseihinsa IAM- järjestelmän piirissä oleville osapuolille. IAM-toimintaympäristön perustoiminnallisuuksiin kuuluu käyttövaltuuksien hallintajärjestelmä sekä siihen liittyvä keskitetty käyttäjä- ja valtuustietovarasto. Valtiovarainministeriön (VM) (2006) käyttövaltuushallinnon periaatteet ja hyvien käytännöt suosituksien mukaan käyttäjäidentiteetin ja käyttövaltuuksien hallintajärjestelmässä keskeisiä osia ovat: 1) automaattinen luvitusprosessi eli käyttövaltuuksien haku- ja hyväksyntä; 2) keskitetty käyttäjä- ja käyttövaltuustietovarasto; 3) automaattinen käyttövaltuustietojen provisiointijärjestelmä sekä; 4) jäljitettävyys-, valvonta ja raportointitoiminnot. (VM 2006A, 24.)

Vuodesta 2009 lähtien Vantaan kaupungin organisaatiossa on ollut käytössä käyttäjähallintajärjestelmä, joka pystyy luomaan, päivittämään ja poistamaan joidenkin järjestelmien käyttäjätunnuksia henkilöstöhallinnonjärjestelmän tietojen perusteella. Järjestelmällä ei ole toteutettu automatisoitua käyttöoikeushallintaa. Ennen nykyistä toimintatapaa järjestelmien tunnuksia koskevat luonti- ja poistopyynnöt hoidettiin manuaalisesti ja järjestelmäkohtaisesti lomakkeita käyttäen. Vantaan kaupungilla on harkittu laaja-alaisemman käyttäjänhallintajärjestelmän ja kertakirjautumisjärjestelmän (SSO, Single Sign On) käyttöönottoa.

3.1.1 Automaattinen luvitusprosessi

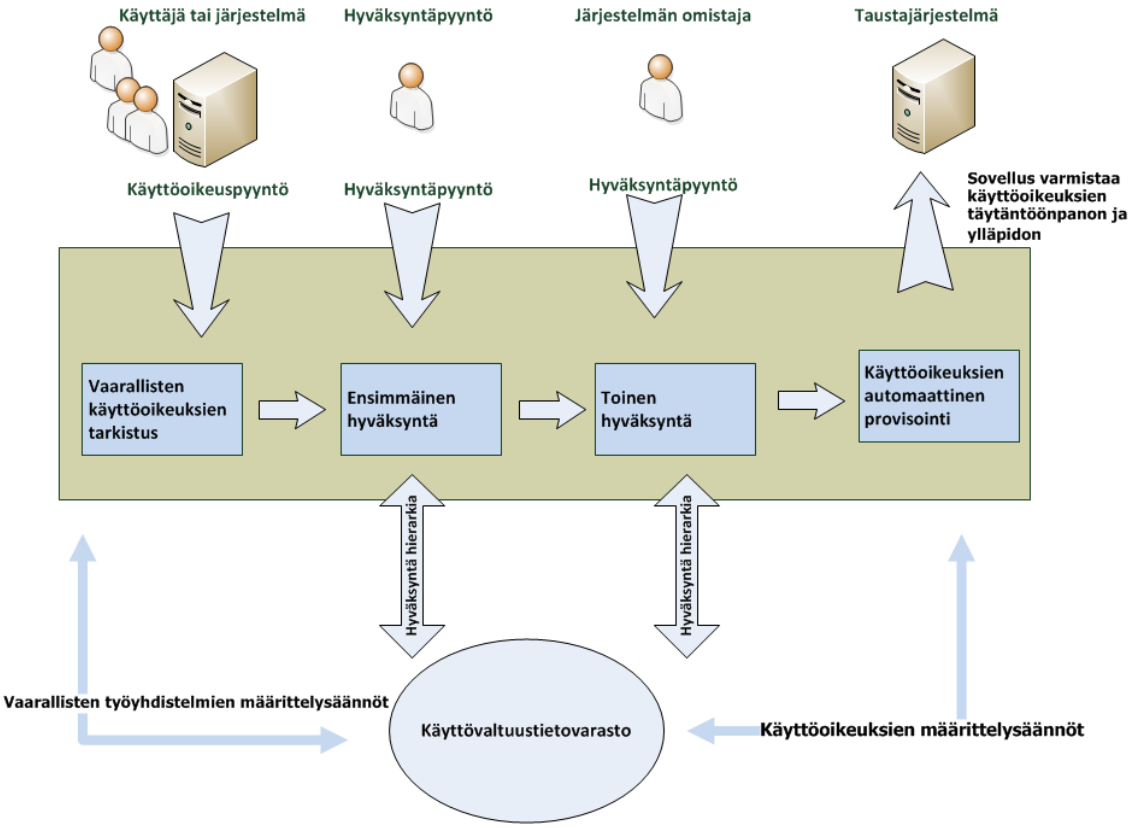
Käyttövaltuushallintajärjestelmän avulla toteutetaan automatisoitu käyttövaltuuksien haku-, hyväksymis- ja luontiprosessi, joka saa syötteensä joko henkilötietoja ja niiden muutoksia käsitteleviltä taustajärjestelmiltä tai muutostietoja itsepalveluna syöttäviltä käyttäjiltä. VM (2006A) mukaan käyttövaltuushallintaprosessien automatisointiin kuuluu toiminnallisuuksien määrittely, jonka ohjaamana käyttövaltuuksien haku-, määrittely- ja hyväksymisprosessi etenee. Käyttöoikeustapahtumiin liittyvät jäljitettävyysvaatimukset, lokijärjestelmä- ja lokien seurantatoiminnot pitää ottaa huomioon osana prosessimäärittelytyötä. Prosessien osana on määriteltävä myös käyttöoikeustapahtumiin liittyvät jäljitettävyysvaatimukset täyttävä lokijärjestelmä ja lokien seurantatoiminnot. Itsepalvelutoiminnan avulla käyttäjät ja heidän esimiehensä voivat hakea tai hyväksyä ennalta määritetyn hallintaprosessin mukaisesti järjestelmän käyttäjätunnuksia ja –oikeuksia. Käyttäjille annetaan käyttöoikeus hallintajärjestelmän kautta. Penn State Uinversty:n (2008) vuoden raportin mukaan IAM:n automatisoinnilla ja rooliin perustuvalla käyttäjien hallinnalla pystytään nostamaan asiakaspalvelua, tietoturvallisuutta sekä lisäämään tuottavuutta. (VM 2006A, 25; Penn State Universty 2008.)

Rai ja muut (2007) täytäntöönpano sisältää todennuksen, luvan ja identiteettien käyttöön lokitietojen saattavuuden kaikista järjestelmistä. Käyttöoikeuksien täytäntöönpano ensisijaisesti tapahtuu automatisoitujen prosessien tai mekanismien kautta. Organisaation palveluksessa olevien käyttäjien perustiedot, käyttäjien asema tai toimenkuva organisaatiossa ja niiden perusteella myönnettävät käyttöoikeudet sekä virka-asema voidaan synkronoida henkilöstöhallintojärjestelmän ja käyttövaltuuksien hallintajärjestelmän välillä. Henkilöstöhallinnon järjestelmästä saatujen tietojen pohjalta voidaan luoda uusi käyttäjä sekä päivittää muuttuneet tiedot. Käyttäjiltä, joiden työsuhde on päättynyt, estetään heidän käyttäjätunnuksiensa käyttö ja poistetaan heidän toimienkuvansa perusteella annetut käyttöoikeudet. Organisaation ulkopuolelta tulevien käyttäjien osalta voidaan lähdetietojärjestelmänä käyttää jotain muuta erillistä rekisteriä. (VM 2006A, 25; Rai ja muut 2007, 5.)

3.1.2 Käyttövaltuustietojen provisiointi kohdejärjestelmiin

Käyttäjäidentiteettien ja käyttövaltuuksien hallintajärjestelmän tehtävä on huolehtia uusien ja muuttuneiden käyttäjä- ja käyttövaltuustietojen automaattisesta provisioinnista kohdejärjestelmiin. Hallintajärjestelmän käyttöoikeushaku- ja hyväksyntäprosessien läpi kulkeneet käyttäjätunnus- ja käyttöoikeuspyynnöt siirretään automaattisesti kohdejärjestelmiin joko heti niiden synnyttyä tai ajastettuna. On suositeltavaa käyttöoikeuden haku- ja hyväksyntäprosessin valvonnan ja ajan tasalla pitämisen kannalta, että tietoa siirretään myös toiseen suuntaan operatiivisesta tietojärjestelmästä käyttövaltuuskantaan. Tietojen siirtoa molempiin suuntiin hyödynnetään vertaamalla käyttövaltuuskannan ja tietojärjestelmissä olevien valtuustietojen tilannetta sekä tavoitteena todeta mahdollisimman reaaliaikaisesti virallisen prosessin ohi annetut käyttöoikeudet ja provisioinnissa tapahtuneet mahdolliset tekniset virheet. Käyttöoikeushaku- ja hyväksyntäprosessin määrittelyssä on otettava huomioon, että käyttövaltuustietoihin sisältyvät käyttäjäidentiteettitiedot ovat henkilötietoja ja niitä koskevat mm. henkilötietolain asettamat velvoitteet. (VM 2006A, 26.)

Käyttöoikeushallinta provisiointiprosessiin kuuluu käyttäjätietojen luominen, muutos, päättäminen, validointi, hyväksyntä, käyttöoikeuksien lisääminen ja viestintä (kuvio 4). Tämä prosessi vaihtelee laajuudeltaan ja kestoajaltaan sekä sen toteutus perustuu organisaation tarpeen mukaan. Prosessia pitää ohjata organisaatio tasolla ja yleisesti sovellettu tietoturva poliittisena linjauksena, joka on kirjattu organisaation liiketoimintayksikön tarpeen perusteella sekä ylläpidetään IT-osaston toimesta. (Rai ja muut 2007, 5.)



Kuvio 4: Loogista automatisoitua käyttöoikeusprovisiointia mukaillen (Rai ja muut 2007, 8)

3.1.3 Jäljitettävyys- ja raportointitoiminnot

Vmk:n suositus (2006A) korostaa, että ”käyttövaltuuksien hallintajärjestelmän keskeinen vaatimus on, että kaikkien sen piirissä olevien tietojen ja tehtyjen tapahtumien tulee olla seurattavissa ja raportoitavissa”. Käyttäjäroolin ja suojattavan kohteen käyttöoikeusvaatimusmäärittelyä tehtäessä pitää ottaa huomioon, että kaikkien muutostapahtumien on oltava jäljitettävissä ja raportoitavissa. Sekä kaikki käyttöoikeuden haku- ja hyväksyntäprosessien tapahtumat että hallintajärjestelmässä suoraan tehdyt tapahtumat tallennetaan lokitietona. Lokitietojen perusteella voidaan seurata käyttäjätietojen ja käyttövaltuuksien muutoksia. (VM 2006A, 26–27.)

Rao, Gupta & Upadhyaya:n (2007) mukaan lokien käsittelyn elinkaareen kuuluvat lokien kerääminen, analysointi, säilyttäminen, luovuttaminen ja poistaminen sekä lokitietojen arkistointi. Hallintajärjestelmäraportin avulla voidaan seurata yksittäisten käyttäjien identiteettejä. Käyttäjän käyttövaltuuksista voi saada milloin tahansa ajantasaisen raportin. Raportista on ilmettävä aktiivisten käyttäjien lisäksi myös passiiviset käyttäjät ja heidän käyttöoikeutensa. Passiiviset käyttäjät ja käyttöoikeudet on oltava helposti havaittavissa ja poistettavissa. (Rao, Gupta & Upadhyaya 2007; VM 2009.)

3.1.4 Tietosuoja ja henkilötietolaki

Identiteetti- ja pääsyhallintajärjestelmää kehittäessä pitää suunnitella, miten huolehditaan käyttäjänidentiteetin tietosuojasta lähtökohtana Suomen henkilötietolaki (22.4.1999/523). Identiteetti- ja pääsyhallintajärjestelmien tietokannassa olevia käyttäjän tietoja on käsiteltävä henkilötietolakia noudattaen. Järjestelmästäkin on tehtävä tietosuoja- ja rekisteriseloste.

Henkilöstälain mukaan henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Tätä lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Myös muuhun henkilötietojen käsittelyyn sovelletaan tätä lakia silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. Identiteetti- ja pääsyhallintajärjestelmää kehittäessä pitää noudattaa seuraavia tietosuojaperiaatteita ja tietosuojadirektiivejä. (Henkilötietolaki 22.4.1999/523, 1 §.)

Henkilötietolaista seuraa rekisterinpitäjälle vaatimuksia, joiden noudattamatta tai toteuttamatta jättämisestä voi olla rikosoikeudellisia seuraamuksia: 1) huolellisuusvelvoite henkilötietojen käsittelyssä; 2) henkilötietojen käsittelyn suunnittelu ja käyttötarkoitussidonnaisuus; 3) henkilötietojen virheettömyysvaatimus; 4) henkilötietojen käsittelyn tarpeellisuusvaatimus; 5) rekisteröidyn informointi tietojen käsittely; 6) rekisteröidyn tarkastusoikeus; 7) rekisteriselosteen laatiminen ja ajantasallapito; 8) tietosuojaviranomaisten tiedonsaanti- ja tarkastusoikeus; 9) virheellisen tai vanhentuneen tiedon korjaamis- tai poistovelvoite; 10) rekisteröidyn kielto-oikeus tietojen käyttämisestä esimerkiksi suoramainontaan; sekä 11) tietojen suojaamisvelvoite. (Henkilötietolaki 22.4.1999/523, 5§– 39 §.)

Yllä mainitun lisäksi on mahdollista, että maistraatti on määrännyt väestörekisterikeskuksen varmennepalveluista annetun lain (661/2009) 4 luvun 36 §:n mukainen rekisteröidylle asianomaisen pyynnöstä määräaikaisen turvakiellon, jolla rajoitetaan hänen yhteystietojensa käsittelyä ja luovuttamista. (Laki väestörekisterikeskuksen varmennepalveluista 21.8.2009/661, 4, 36§.)

3.1.5 Omatoiminen IAM- ratkaisuihin tutustuminen

Vuonna 2012 syksyn puolivälissä julkaistun Management Events:in tutkimuksessa kysyttiin 33 organisaatiolta, miten identiteetin ja käyttövaltuuksien hallintaan liittyvät investoinnit tulevat kehittymään seuraavien 18 kuukauden aikana. Vastaajista 73 % oli sitä mieltä, että investointien kehitys on kasvava ja 24 % arvioi kehityksen pysyvän nykyisellä tasolla. Tämän tutkimuksen tekijän mielestä edellä mainittu tutkimus osoitti, että organisaatiot ovat sisäistäneet IAM- hankkeen osana organisaation strategian toteuttamista ja liiketoiminnan kehittämistä. Konfrensissa, jossa em. tutkimuksen tulokset esiteltiin, IAM- hankkeeseen esitettiin kuuluvaksi

tehtävien ja vastuiden määrittely, toteutuksen suunnittelu, työnkulku ja prosessien kuvaaminen, riskien analysointi, IAM-järjestelmän toteutuksesta saatavien hyötyjen ja saatujen kokemusten arviointi. (Management Event conference 2012.)

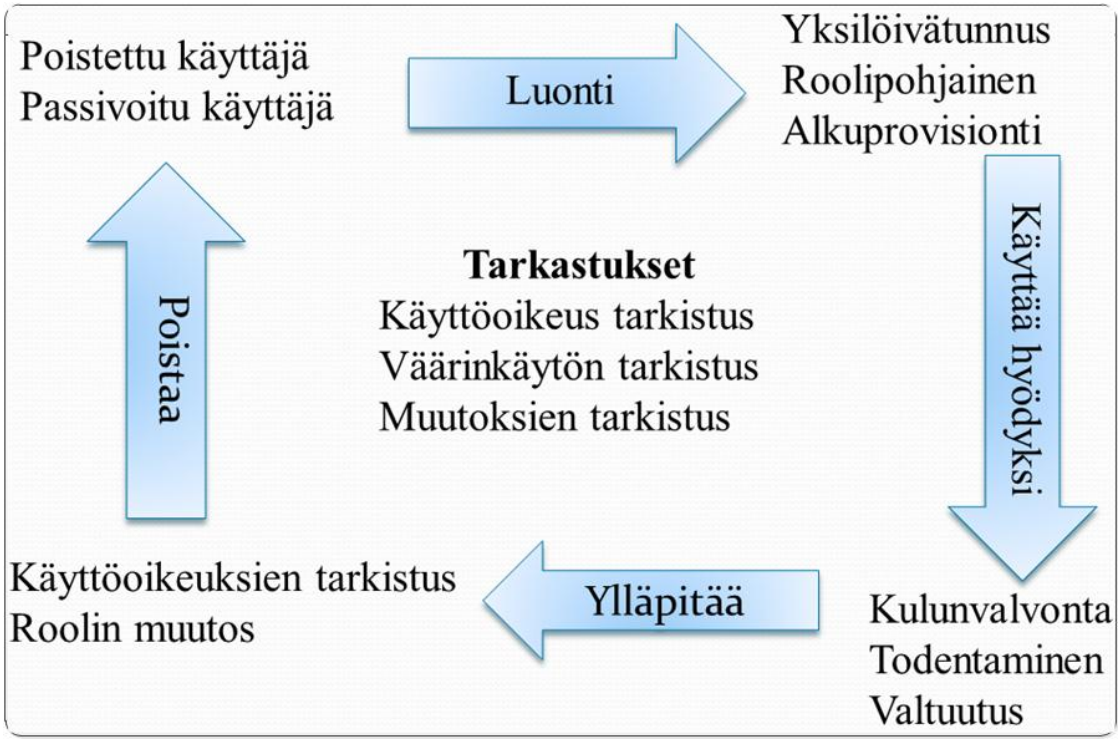
Nykyään IAM- ratkaisuja on tarjolla runsaahkosti. Tutkimuksen tekijä on tutustunut taulukossa 3 mainittuihin markkinoilla tarjolla oleviin IAM- ratkaisuihin.

Tarjoaja	Tuote
SailPoint	IdentityIQ Lifecycle Manager
CA technologies	CA Identity Manager
IBM	Tivoli Identity Manager Software
Oracle	Oracle Identity Management
RM5 Software Oy	RM5 IdM Entitlement Management Software
SAP	NetWeaver Identity Management
Ubisecure	Ubisecure CustomerID
Microsoft	Forefront Identity Manager 2010 R2

Taulukko 3: Markkinoilla tarjoilla olevat IAM- ratkaisut, joihin tutkimuksen tekijä on tutustunut

3.2 Käyttövaltuushallinnon hallintaprosessi

VM:n (2006A) suosituksen mukaan käyttövaltuushallintaprosessin toimintoihin kuuluvat tietojärjestelmät, käyttäjät, käyttöoikeudet sekä käyttövaltuuksien ylläpito. Lisäksi organisaation tietoturvapolitiikan toteuttaminen käytännössä edellyttää käyttövaltuushallintaa ja siihen liittyviä prosesseja koskevan politiikan laatimista. Käyttövaltuuksien hallintapolitiikassa määritellään organisaation käyttövaltuusperiaatteet ja niiden toteuttamiseksi noudatettavat toimintatavat. Organisaation prosessien toteutustapa pitää pyrkiä saamaan yhdenmukaisiksi koko organisaatiossa. Käyttövaltuushallintaprosessit suunnitellaan siten, että ne kattavat kaikkien käyttövaltuushallinnan kohteiden elinkaaret ja varmistetaan, että ne ovat riittävän turvallisia (kuvio 5). Toteutusprosessin kuvaukset sekä ohjeistukset on pidettävä ajantasalla sekä jokaiselle prosessille on nimettävä vastuuhenkilö yhteystietoineen. Näiden prosessien vastuuhenkilöiden velvollisuudet ja valtuudet on määriteltävä selkeästi. Suojattavien kohteiden omistajilla on velvollisuus osallistua käyttövaltuuksien myöntämis- ja poistamisprosessien määrittelyyn. Tällä tavalla omistajataho päättää ja osaltaan vastaa käyttövaltuuksien myöntämisestä ja poistamisesta. Käyttövaltuushallintaprosessissa kaikista käyttöoikeuspyynnöistä ja niiden hyväksyntä tapahtumista on oltava jäljitettävissä tieto käsittelijöistä ja tapahtumien ajankohdasta. (VM 2006A, 26–29; Rai ja muut 2007.)



Kuvio 5: Identiteetin hallinta elinkaarta mukailen (Rao, Gupta & Upadhyaya 2007, 209)

VM:n Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) (2006A) -ohjeessa on kiinnitetty huomiota erityisesti siihen, että hallintaprosessien toteutuksessa otetaan huomioon tilanteet, joissa käyttäjän työsuhde on päättynyt tai hänen työroolinsa (Business role) muuttuu siten, että se vaikuttaa käyttövaltuuksiin. Tällöin on huolehdittava siitä, että työnantajan palveluksesta poistuneen käyttäjän käyttäjätiedot ja kaikki siihen liittyneet käyttäjätilit ja käyttövaltuudet tai käyttäjän aikaisempaan rooliin liittyvät uutta tilannetta vastaamattomat käyttövaltuudet poistetaan. Historiatiedon on kuitenkin säilyttävä ennalta määritelty ajanjakso, joka riippuu osin asianomaisten järjestelmien tukeman toiminnan luonteesta esim. maksujärjestelmät, kirjanpito, päätöksentekojärjestelmän. (VM 2006A, 29.)

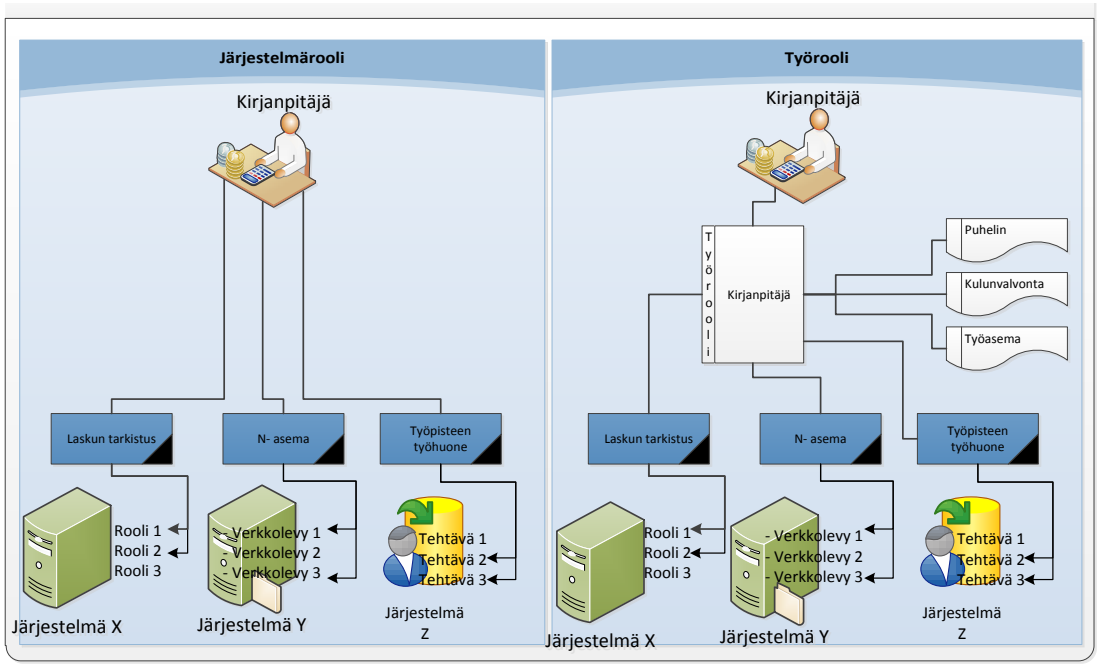
Vantaan kaupungin organisaatiossa on käytössä itsepalveluportaali, jolla esimiehet pystyvät hakemaan eri järjestelmien käyttöoikeuksia alaisilleen. Itsepalveluportaalia käytetään käyttäjätunnuksien ja käyttöoikeuksien hakua ja hyväksyntää varten. Itsepalveluportaalia ei ole integroitu muihin taustajärjestelmiin, joten haetut ja hyväksytyt käyttöoikeudet eivät siirry (provisoidu) automaattisesti taustajärjestelmiin. Kun hyväksyjä tai esimies on hyväksynyt jonkin käyttöoikeuden lisäämisen tai poiston, kyseessä olevan tietojärjestelmän pääkäyttäjä lisää manuaalisesti käyttöoikeuden ko. järjestelmään tai poistaa sen järjestelmästä. Itsepalveluportaalin lisäksi käyttöoikeutuspyynnön tekemiseksi on käytettävissä mm. pdf-lomake, paperinen lomake ja sähköpostijärjestelmä.

VAHTI-ohjeessa VM (2006A) todetaan, että itsepalveluportaalista on saatava raportti siitä, kuka on hakenut käyttöoikeutta sekä kuka on hyväksynyt ja käsitellyt käyttöoikeuspyyntöä. Manuaalisella (itsepalvelun ulkopuolella) keinolla haetut käyttöoikeuksien raportin saaminen on haastavaa ja työlästä. (VM 2006A, 29.)

3.2.1 Käyttäjärooli (käyttäjäryhmä)

VM (2006A) suosittelee, että käyttövaltuuksia määriteltäessä ei ole käytännöllistä eikä järkevää tarkastella käyttäjiä yksilötasolla, vaan tulee pyrkiä löytämään käyttäjäryhmiä, joiden jäsenillä on samantyyppiset työtehtävät. Näin ollen heillä on samanlaiset tietotarpeet ja toimintavaltuudet eli samanlainen toiminnallinen rooli, jota tässä kutsutaan työrooliksi. Käyttövaltuushallinnon kannalta päästään tehokkaampaan ja joustavampaan lopputulokseen erottamalla toisistaan käyttäjien työroolit ja palvelujärjestelmien mahdollistamat käyttäjäroolit. Rao, Gupta & Upadhyaya (2007) korostavat, että eräs tapa hallita käyttäjien käyttöoikeuksien valtuuksia on käyttää roolipohjaista käyttöoikeushallinta Role Based Access Controlia (RBAC). Roolipohjainen käyttöoikeuksien hallinta on tapa jakaa käyttövaltuuksia käyttäjille, jotka perustuvat työtehtäviin tai rooliin kyseisessä organisaatiossa. Se helpottaa uuden käyttäjän liittämisen niihin ryhmiin, jotka sisältävät kaikki käyttövaltuudet käyttäjän työtehtäviin. Roolipohjaista käyttöoikeushallintaa käyttämällä saavutetaan useita etuja: 1) yksinkertaistaa tietoturvaa ryhmittelemällä käyttövaltuuksia loogisesti perustuen työtehtävien rooleihin organisaation sisällä; 2) vähentää esimiehien käyttöoikeuksien hakemiseen kuluvaa aikaa ja vaivaa uusia työntekijöitä palkattaessa sekä; 3) parantaa käyttöoikeustarkastusta antamalla yksityiskohtaista tietoa käyttövaltuuksien tarkistuksessa. Schaad, Moffett, & Jakob (2001) viittaavat Sandhu, Ferraiolo, & Kuhn (2000) Rooli-pohjainen pääsynvalvonta on hyvin määritelty tutkimusalue, jossa tehdään jatkuvaa työtä määritettelemällä rooli-pohjaisen käyttöliittymän valvonnan standardia. (VM 2006A, 17–18; Rao, Gupta, & Upadhyaya 2007; Schaad, Moffett, & Jakob 2001; Sandhu, Ferraiolo, & Kuhn 2000; Pulman & Streff 2008.)

Järjestelmäroolin ja työroolin välillä on eroja roolin käyttötarkoituksessa (kuvio 6). Järjestelmäroolin tarkoitus on määritellä kyseessä olevan järjestelmän sisälle käyttöoikeus, joka mahdollistaa tehdä tietyn tehtävän suorittamisen tässä järjestelmässä. Järjestelmärooli voi olla esimerkiksi taloushallinnon järjestelmässä laskun asiatarkistaja, laskun hyväksyjä tai järjestelmän ylläpitäjä. Näitä rooleja ylläpidetään kyseessä olevassa järjestelmässä ja kytketään käyttäjille samassa järjestelmässä.



Kuvio 6: Käyttäjälle kytkettyjen järjestelmäroolin ja työroolin eroavaisuus

Työrooli on koosterooli. Se koostuu henkilön työtehtävistä, organisaationhierarkiasta, työpisteestä tai asemasta. Työroolin näkökulma on työntekijän työtehtävissään tarvitsemat käyttöoikeudet. Työroolin käyttöoikeuksien sisällössä voi olla erilaisia sovellusrooleja, tietojärjestelmärooleja, käyttäjäryhmiä tai asemaan liittyviä käyttöoikeuksia järjestelmiin, fyysisiä käyttöoikeuksiin tai jonkin laitteen käyttölupa esim. puhelin tai kulunvalvontalaitteisto. Työroolilla pystyy työskentelemään erilaisissa organisaation käytössä olevia järjestelmiä käyttäen. Kuvassa 4 on pyritty kuvaamaan miten järjestelmärooli ja työrooli eroavat toisistaan. Työrooleja ylläpidetään IAM- järjestelmässä. Järjestelmäroolien sisällön tai laajuuden muuttuessa muutos siirtyy ajantasaisesti työrooleihin. Tämän työn kirjallisuustarkastelu sisälsi seuraavia keskeisiä käyttäjäroolitutkimuksia. (VM 2006A, 17–19; Schaad, Moffett & Jakob 2001; Rao, Gupta & Upadhyaya 2007; Sandhu, Ferraiolo, & Kuhn 2000; Rai ja muut 2007.)

3.2.2 Käyttövaltuutuksien määrittely

VM (2006A) mukaan käyttövaltuuksien määrittely tarkoittaa käyttöoikeuksien kytkemistä käyttäjien työrooleihin. IAM- palvelujärjestelmien käyttöoikeudet tai osa niistä saattaa olla koottu joukoksi järjestelmän rooleja, joihin työroolit kytketään siten, että halutut käyttövaltuudet syntyvät. Jos rooleja ei ole määritelty järjestelmään, niin työrooleihin kytketään asianmukaiset yksittäiset käyttöoikeudet. (VM 2006A, 20.)

Esimies tai järjestelmän omistaja määrittelee ja viime kädessä hyväksyy kenelle ja millä ehdoilla käyttövaltuuksia myönnetään. IAM- hallintajärjestelmässä, jossa käyttövaltuudet ovat työroolikohtaisia, työroolin omistajan tehtävänä on hankkia työroolille sen edellyttämät käyttövaltuudet sopimalla asiasta ao. kohteen omistajien kanssa. Pääperiaatteena työroolin käyttövaltuuksien määrittelyssä tulee pitää todellista tarvetta, toisin sanoen rooliin ei tule kiinnittää kaiken varalta laajempia valtuuksia, kuin mitä rooli käytännössä edellyttää. Tilapäiset, normaalitarvetta laajemmat tiedonkäsittely- tai pääsyoikeudet tai muut käsittelyvaltuudet tulee hoitaa käyttäjälle esimerkiksi määräajaksi aktivoitavalla työroolilla, johon on liitetty tarvittavat määräaikaiset valtuudet. Uuden työntekijän tullessa organisaatioon hänet liitetään aloitustoimenkuvaansa vastaaviin työrooleihin. Työuransa aikana hänet lisätään tarpeen mukaan uusiin rooleihin ja irrotetaan entisistä rooleista, jotka eivät enää vastaa hänen uusiutunutta toimenkuvaansa ja sen edellyttämiä valtuuksia. (VM 2006A, 20–23.)

Rao, Gupta & Upadhyaya (2007) korostavat, että eräs vaihe identiteetin hallinnan elinkaaressa on käyttäjätilin hyödyntäminen. Kun käyttäjä on valmis aloittamaan työt, hänet on ensin todennettava järjestelmään hänen käyttäjätunnuksella ja salasanalla tai jollain muulla varmennusmenetelmällä. Todentamisprosessia on vahvistaa käyttäjän henkilöllisyys, koska vain omistaja tietää käyttäjän tilin ja salasanan. Todentamisen jälkeen, käyttäjällä on oikeus suorittaa jokin toiminto, kuten käyttöoikeus hyväksyntähakemus. Lupamenettelyprosessi luottaa käyttäjän henkilöllisyyteen, koska käyttäjä on päässyt läpi todentamalla tunnuksen ja salasanan. Tämän jälkeen tarkistetaan, että käyttäjällä on annettu valtuus erilaisiin toimintoihin tai käyttöoikeuksiin hänen tunnuksillaan. Eli todentamisen ja valtuutuksen ero on, että todentaminen (Authentication) on prosessi, joka sallii käyttäjän järjestelmään ja valtuutuslupa (Autorization) varmistaa, että käyttäjällä on oikeus käyttää resursseja tai suorittaa toimintoja järjestelmässä. (Rao, Gupta & Upadhyaya 2007, 208–240.)

3.2.3 Käyttövaltuuksien muutos ja myöntäminen

Rao, Gupta & Upadhyaya (2007) puolestaan kuvaavat Identiteetin hallinnan elinkaaren ensimmäinen vaihe on käyttäjätilin luonti. Käyttäjän tieto voi olla aluksi luotu osaksi henkilöstöhallinnan HR- järjestelmässä. HR- järjestelmän tietojen perusteella luodaan eri järjestelmien käyttäjätilejä. Kun ensimmäiseksi käyttäjätili on luotu, sille lisätään vain oikeuksia, joita tarvitaan käyttäjän työtehtävän mukaisesti. Käyttäjätili on ainutlaatuinen yksilö ja käyttäjätilejä ei pidä jakaa kenellekään. (Rao, Gupta & Upadhyaya 2007, 208–240.)

VM (2006A) mukaan kaikki käyttövaltuuksien muutokset tulee tehdä ennalta määritellyn prosessin mukaisesti niin, että muutokset ovat myöhemmin jäljitettävissä. Työroolin kytkentä tietojärjestelmän rooliin tai yksittäiseen käyttöoikeuteen edellyttää asianomaisen kohteen omistajan hyväksyntää. Käyttäjän liittäminen työrooliin edellyttää vastaavasti työroolin omis-

tajan hyväksyntää. Jos työrooliin kuuluu käyttövaltuuksia, joihin liittyy erityisehtoja kuten käyttäjän tietynlainen rekisteröintitapa tai tietynlaisten tunnistusvälineiden käyttö, nämä on otettava huomioon kytkettäessä käyttäjää ao. työrooliin. Hyväksyjän pitää kuitenkin varmistaa, että kyseinen työrooli on käyttäjän työkuvaa vastaavalla tasolla sekä ei aiheuta vaarallisia työyhdistelmiä. (VM 2006A, 24-5.)

3.2.4 Käyttövaltuuksien valvonta

Vmk:n VAHTI-suosituksen mukaan käyttövaltuuksien valvonnan tarkoituksena on seurata, että 1) sovittuja käytäntöjä noudatetaan; 2) käyttäjä- ja valtuustiedot ovat ajan tasalla sekä; 3) hallinta- ja palvelujärjestelmiin ei kerry tarpeettomiksi käyneitä vanhoja määrityksiä.

Valvonnan perustana ovat hallintajärjestelmän lokitiedot sekä hallinta- ja palvelujärjestelmissä olevat käyttäjä- ja käyttövaltuustiedot. Valvonnan välineitä ovat erilaiset raportointivälineet sekä säännölliset katselmoinnit. Valvonnan ovat velvollisia järjestämään kyseessä olevien tietojen vastuulliset omistajat, eli työroolit omistavat organisaatioyksiköt sekä suojattavien kohteiden omistajat. (VM 2006A, 25–26.)

Identiteetin hallinnan elinkaaren vaiheessa tarkastusvaiheella on merkittävä asema. Käyttäjätilien tarkastusvaihe pitää toteutua kaikissa identiteetin elinkaaren vaiheissa. Kun käyttäjätili on ensin luotu, jonkinlainen asiakirja tulee tallentaa, jotta osoitetaan miksi käyttäjätili luotiin. Käyttäjälle myönnetyt käyttöoikeudet voidaan tarkistaa sen varmistamiseksi, että ne ovat oikein ja prosessin mukaiset. Käyttäjätilin käyttöaikana järjestelmän lokitiedostoja on voitava tarkistaa, ettei järjestelmän käyttöä ole rikottu sekä ettei sillä ole pääsyä kriittisiin resursseihin. Kun tili on poistettu, järjestelmä pitää tarkastaa sen varmistamiseksi, etteivät käyttöoikeudet, jotka ovat liitetty käyttäjätiliin säily järjestelmässä. Tarkastus on osa tehtävää, joka on sidottu käyttäjätilien ylläpitoon. Kaikkien käyttäjätilien käyttöoikeudet pitää tarkistaa säännöllisesti. (Rao, Gupta & Upadhyaya 2007, 208–240.)

3.2.5 Käyttöoikeuksien sisältö ja laajuus

Vantaalla esimiehet hakevat käyttöoikeuksia alaisilleen, jotta alaiset voivat käyttää heidän työkuvansa vaatimia tietojärjestelmiä. Tätä tarkoitusta varten luodussa itsepalveluportaalissa on erilaisia lomakkeita (pääkäyttäjä, esimies ja loppukäyttäjä), joihin liittyville toiminnoille on eritasoisia käyttöoikeuksia. Kaikkien lomakkeissa olevien käyttöoikeuksien osalta ei ole kuvattu miten laajoja ne ovat ja mistä ne koostuvat. Lisäksi itsepalveluportaalista ei ole mahdollista saada raporttia esimiesten alaisten käytössä olevista kaikista käyttöoikeuksista. Vahdin ohjeissa kuvaillaan käyttöoikeuksien hallinnan ongelmia, kun käyttöoikeuksien hallin-

nassa prosesseja ja vastuita ei ole kuvattu tarkasti. Käyttöoikeuksien myöntämisen prosessia ei kontrolloida kunnolla ja henkilöille annetaan varmuuden vuoksi liian laajat oikeudet. Tällaisia ongelmia syntyy sekä perinteisessä manuaalisessa, että itsepalvelua hyödyntävässä käyttöoikeushallinnassa. (VM 2006A, 23–28.)

Käyttäjätilien ylläpito on yksi käyttäjähallinnan merkittävimpiä asioita elinkaaren aikana. Jokaisen organisaation muutoksen pitää heijastua myös käyttäjätileihin. Jos organisaatio luo uuden tyyppisen käyttöoikeuden, koko käyttöoikeusprosessi sisältöä tai rajauksen hyväksyntäkäytäntöä pitää tarkistaa koko IAM- järjestelmän läpi. Käyttäjän käyttäjätunnuksella on voitava käyttää uusia toimintoja. Kun käyttäjän työkuva muuttuu, käyttäjätiliin täytyy lisätä, muuttaa tai poistaa, myös työntekijöiden muuttuvia rooleja uuden järjestelmän tai liiketoiminnan resursseja vastaavaksi ja vanhentuneet järjestelmäroolit tai resurssit poistetaan. (Rao, Gupta & Upadhyaya 2007, 210.)

Rai ja muut (2007) Gartner IAM- tutkimuksessa nostetaan esille, että tehokas IAM- ratkaisu pyrkii vastaamaan seuraaviin kolmeen kysymykseen: 1) Kenellä on oikeus mihinkin tietoihin? Hyvä IAM- järjestelmä tukee organisaation digitaalista identiteettihallintaa. Lisäksi järjestelmä pystyy myös hallitsemaan näiden identiteettien pääsyä resursseihin, sovelluksiin ja suojattuun informaatioon; 2) Vastaavatko käyttöoikeudet työtehtäviä? Käyttöoikeuksien määrittelyssä pitää ottaa huomioon, että ne vastaavat työtehtävää sekä tarkistaa, että käyttöoikeus ei tuota mahdollisia vaarallisia työyhdistelmiä; 3) Seurataanko käyttöoikeusprosessia, lokitetaanko sekä raportoidaanko sitä suunnitelmallisesti? IAM- prosessia kuvattaessa pitää suunnitella sen säännöllinen seuranta ja valvonta. Käyttöoikeudet pitää määritellä, kirjata, dokumentoida, valvoa käyttöä, sekä raportoida asianmukaisesti. (Rai ja muut, 2007, 3.)

3.3 Vaarallisten käyttöoikeuksien yhdistelmä

Eräs keskeisistä tietoturvamekanismeista on vaarallisten työyhdistelmien tunnistaminen ja niiden syntymisen estäminen. Vaarallinen työyhdistelmä (Segregation Of Duties, SOD) tarkoittaa, että henkilö itse sekä suorittaa, että hyväksyy tekemänsä tapahtumat tai tilanteet, joissa vain yksi tai muutama henkilö hoitaa kriittisen prosessin ilman riittävää valvontaa. (Compliance Tutorial 2008.)

Spaffordin (2006) mukaan perustavoite tehtävien eriyttämisen valvonnalle on, ettei kenellekään tulisi liikaa valtaa yhteen tai useampaan kriittiseen prosessiin. Vaarallisten työyhdistelmien tunnistamismenetelmällä pystyy erottamaan roolit ja vastuut sekä varmistamaan, että henkilö ei voi käsitellä organisaation liiketoiminnan kannalta kriittisiä toimintoja ilman toisten osallistumista ja sitä kautta vähentämään väärinkäytöksen mahdollisuutta. (Spafford 2006.)

Vantaan kaupungin sisäinentarkastus suoritti taloushallinnon vaarallisten rooliyhdistelmien tarkastuksen, jossa tarkastuksen painopiste oli tuolloin uudehkossa toiminnanohjausjärjestelmässä. Organisaation vaarallisten työyhdistelmien määrittelytarve on raportin mukaan suppea eli vähäinen. Vantaalla on tehty määrittely vaarallisista rooliyhdistelmistä taloushallinnon osalta. (Vantaan sisäinen tarkastuskertomus 2011.)

Deloitte:n (2006) mukaan keskeisimpiä haasteita, jotka aiheuttavat vaarallisia työyhdistelmiä ovat: 1) ei ole määritelty tietoturvapolitiikkaa, tietoturvapolitiikka on liian suppea ja vastuiltaan epäselvä tai tietoturvapolitiikka on, mutta sen toteutumista ei seurata tai valvota; 2) organisaation johdon tuen puuttuminen; 3) tietoturvapolitiikka ei ole riittävästi kytketty osaksi liiketoimintastrategiaa tai se on hajautunut (esim. organisaatiossa erilaisia ja epäyhtenäisiä tietoturvakäytäntöjä); 4) puutteellinen tiedottaminen sekä esimies- ja käyttäjäkoulutus vaarallisista työyhdistelmistä sekä niiden välttämiseksi huomioitavista seikoista; 5) riittämättömät tietoturvakäytännöt ja käyttöoikeushallintamenettelyt, joilla pystyttäisiin hallitsemaan tilanteet, jotka syntyvät käyttäjien työtehtävien muuttuessa tai heidän lähtiessään organisaatiosta; 6) rajoitetut automaattisen raportointivalmiudet eri järjestelmien käyttöoikeuksien valvonnalle suhteessa käyttäjien työtehtäviin sekä; 7) puutteelliset seurantavälineet käyttöoikeuksien tarkastamiseen ja kyky tarkastella vuosikelloittain. (Deloitte 2006.)

Tirrosen (2003) mukaan vaarallisten työyhdistelmien syntymistä pyritään estämään siten, että yksi työntekijä ei ole vastuussa kahdesta toisistaan riippuvasta työtehtävästä. Khan (2010) tarkentaa, että eräs tärkeä näkökohta vaarallisia työyhdistelmiä analysoitaessa ja tietoturvan toteutumisen seurantaa varmistettaessa on, että organisaatiolla on selkeä käsitys organisaation toiminnalle tärkeistä tiedoista. Lisäksi näiden tietojen tulee olla luokiteltu asianmukaisesti mm. tietojen turvaluokitus, luokiteltujen tietoryhmien käsittelyyn oikeutettujen määrittely, tietojen turvaluokitukseen perustuvat tietojen käsittelyyn osallistuvien roolit ja vastuut, tietojen sensitiivisyys ja kriittisyyden arviointi organisaation toiminnan ja toiminnan jatkuvuuden kannalta. (Tirronen 2003; Khan 2010, 5.)

VM (2006A) korostaa, että työrooleja, joihin liittyy erityisen laajoja käyttövaltuuksia (esim. pääkäyttäjän tai järjestelmävastaavan oikeudet, käyttöjärjestelmän ja niin sanottujen välitason ohjelmien (Middleware) käyttöoikeudet, myöntämisessä tulee käyttää erityistä harkintaa. Niiden käyttöön tulee liittyä käyttövaltuuksien laajuuteen liittyviä erityisehtoja ja -näkökohtia kuten käyttäjän vahva tunnistaminen, käyttötilanteiden määrittely, ohjeet ja käyttäjäsitoumukset. Työrooleja tai työroolien yhdistelmiä, joihin sisältyy vaarallisia tai riskialttiita käyttövaltuusyhdistelmiä, on vältettävä. Jos laajoja oikeuksia on pakko myöntää, niiden käyttöä on valvottava normaalia tarkemmin ja seurattava, että käyttövaltuudet pysyvät työtehtävien muutosten tasalla. Erittäin kriittisten tai erityistä suojausta edellyttävien tietojen ja kohteiden käytössä voi olla tarpeen soveltaa menettelyä, jossa käyttövaltuus

(omistajatahon käyttölupa) haetaan aina kertaluonteisesti yksittäisessä käyttötilanteessa esim. määräaikaisesti voimassa olevana. (VM 2006A, 17.)

4 Käytetyt tutkimusmenetelmät ja vaiheet

Tässä tutkimuksessa on käytetty tutkimusmenetelmänä tapaustutkimusta ja suunnittelutieteentutkimusta. Tässä luvussa on myös käsitelty tapaustutkimusmenetelmän etuja ja haittoja. Tapaustutkimusmenetelmänä on käytetty Yin:in (2009) esittämää tapaustutkimuksen lineaarisen ja iteratiivisen prosessin mukaisesti eli tutkimuksen suunnitelma (plan), toteutuksen suunnittelu (design), tutkimuksen valmistelu (prepare), aineiston kerääminen (collect), tietojen analysointi (analyze) sekä tuloksen jakaminen (share). Kuvio 7.

Suunnittelutieteellisen tutkimusmenetelmän esittämisessä on sovellettu Nunamakerin järjestelmänkehitystutkimusmetodologiaa. Nunamaker, Chen & Purdin (1991) kiteyttävät tietojärjestelmien tieteellisen tutkimusprosessiin kuuluvaksi ymmärtämisen, suunnittelun, kehittämisen, implementoimisen sekä toteutetun järjestelmän tavoitteiden mukaisen toimivuuden tarkistamisen ja arvioimisen. (Nunamaker, Chen & Purdin 1991, 96.)

4.1 Tapaustutkimus

Tapaustutkimuksessa tarkastellaan yhtä tapausta. Tiedonhankintatapoina ovat kyselyt, haastattelut, havainnointi ja arkistomateriaalin käyttö. Kerättävä tieto voi olla sekä määrällistä että laadullista. Yin (2009) puolestaan totea, että tapaustutkimus on jotain ainutlaatuista, erityistä tai mielenkiintoista tarinaa, joka voi koskea yksittäisiä ihmisiä, organisaatioita, prosesseja, ohjelmia, asuinpaikkoja, instituutiota ja jopa yksittäisiä tapahtumia. Yin (2009) viittaa myös Philliber, Schwab, & Samsloss (1980) mukaan eräs tapa ajatella tutkimuksen suunnittelu on kuin toimintasuunnitelma ”blueprint” tutkimukselle, joissa käsitellään ainakin neljää ongelmaa: 1)mitä kysymyksiä tutkitaan; 2) mitkä tiedot ovat merkityksellisiä; 3) mitä tietoja kerätään sekä; 4) kuinka tulokset analysoidaan? (Yin 2009, 26; Philliber, Schwab & Samsloss 1980.)

Thomas (2011) määrittelee tapaustutkimuksen olevan jonkin asian kokonaisvaltaista hahmottamista tarkastelemalla sitä useasta eri näkökulmasta. Tämä monitahoinen tarkastelu edistää todennäköisesti myös objektiivisemman kuvan syntymistä tutkimuskohteesta ja siihen liittyvistä ilmiöistä. Laine, Bamberg & Jokinen (2007) kuvailevat mitä tapaustutkimuksesta on opittavissa. Heidän mielestä tapaustutkimukselle on ominaista, että pyritään selvittämään jotain, mikä ei ole entuudestaan tiedossa ja josta tarvitaan lisää tietoa. Avison, Lau, Myers, Nielsen(1999) viittaavat, että Laun (1997) toimintatutkimuksen avulla voidaan käsitellä monimutkaisia tosielämän ongelmia. Onnistuneessa toimintatutkimuksessa on epätodennäköistä esiintyä ristiriitoja tutkijoiden ja käytännön tai toimijoiden keskuudessa. Lau (1997) ehdottaa tarpeen toimintatutkimuksen monografian samanlaisuudesta. Tapaustutkimusmetodologia koostuu neljästä ulottuvuudesta: 1) käytettyn tapaustutkimuksen luokituksesta ja sen painopisteestä; 2) perinteisen ja uskomuksen epäsuorista oletuksista; 3) tutkimuksen prosessista,

teemasta, osallistujien organisaatioiden tasosta, muutoksen suuruudesta ja tutkijan roolista sekä; 4) hyväksytystä esitystavasta. (Avison, Lau, Myers & Nielsen 1999, 95–97; Lau 1997; Thomas 2011, 23; Laine, Bamberg & Jokinen 2007, 10.)

4.1.1 Tutkimuksen suunnitelma (Plan)

Yin:in (2009) mukaan tutkimusmenetelmän valintaan vaikuttaa kolme seikkaa: tutkimuskohteen tyyppi, tutkijan osallistumisen ja käyttäytymisen laajuus tapahtumaan sekä ajankohtaisiin tapahtumiin keskittyminen suhteessa historiallisiin tapahtumiin. Yin suosittelee, että tutkimusmenetelmän valinnassa avoimuus eri menetelmien suhteen on tärkeää, koska erilaiset menetelmät limittyvät keskenään. (Yin 2009, 8.)

Corbin & Strauss (1998) viittaavat Pattonin (1990) kommenttiin, että laadullisen tutkimuksen arvioinnin tutkijoille, "laadullisen arvioinnin tutkimus pohjautuu sekä kriittisen ja luovaan ajatteluun, sekä tieteen ja taiteen analyysiin". Hän korostaa käyttäytymistapoja, jotka ovat hänen mielestään hyödyllisiä edistämään luovaa ajattelua; Jokaisen analyytikon täytyy pitää mielessä myös: a) olla avoin useille mahdollisuuksille; b) tuottamaan vaihtoehtojen luettelon; c) tutkimalla eri vaihtoehtoja ennen mitä tahansa valintaa; d) hyödyntämään useita ilmaisun keinoja; e) käyttämään epälineaarisia ajattelumuotoja kuten edestakaisin ja kiertää ympäri aihetta saaden tuoreita näkökulmia; f) poiketa omasta tavanomaisesti ajattelutavasta ja työstä saadakseen tuoreita näkökulmia; g) luottaen prosessiin, eikä pidätellä tai jarrutella; h) ei ole oikotietä, vaan tarvitaan paljon työtä sekä; i) pitää hauskaa samalla, kun tekee tutkimusta. Corbin & Strauss (1998) korostavat, että ”analyysi on vuorovaikutusta tutkijoiden ja tiedon välillä. Se on sekä tiedettä ja taidetta”. (Corbin & Strauss 1998, 12–13; Patton 1990, 434–435.)

Patton (2002) puolestaan kuvailee, että laadullisen menetelmän suunnittelussa on kolme erilaista laadullisen datan kerääminen vaihtoehtoa: haastattelu, havainto ja asiakirjat. 1) Haastattelun avulla saadaan vastaus avoimiin kysymyksiin, syvällistä vastausta ihmisten kokemuksesta, käsityksestä, tunteesta sekä tietämyksestä; 2) Havainnolla puolestaan saadaan kenttätyö toiminnan kuvauksia, käyttäytymistä, keskusteluja, ihmissuhteita, vuorovaikutusta sekä organisaation tai yhteisön prosesseja tai muita näkökohtia todettavia ihmisten kokemuksia. Havainnon avulla kerätty aineisto on rikas, yskityskohtainen ja kuvauksellinen; 3) Asiakirjaan kuuluu erilaisia materiaaleja, ohjelmatietueita, muistioita, kirjeenvaihtoja, virallisia julkaisuja, raportteja, kirjeitä ja taiteellinen työ. Hän tarkentaa, että hedelmällisen laadullisen tutkimuksen suunnittelun onnistumiseksi tutkijan on tärkeä tietää, miltä laadulliset tiedot ja havainnot näyttävät niin, että tietää mitä etsii. Samalla on myös tärkeä pohtia laatukriteerit laadullisen tiedon päättelyyn. Yin (2009) selittää laadullinen tutkimussuunnittelu kriteerin arvioimiseksi viittamalla U.S. Goverment Accountability Office, (1990) ja Kidder & Judd (1986) kun laadullinen tutkimuksen suunnittelu on tarkoitus edustaa loogista joukko lausunto-

ja, on olemassa tiettyjä keinoja tai loogisia testejä, jolla voidaan arvioimaan mikä tahansa suunnittelun laatua. Nämä looginen käsitteet ovat: 1) luotettavuus 2) uskottavuus 3) vahvistettavuus sekä 4) tietojen luotettavuus. Kidder & Judd (1986) puolestaan selittää nämä oppikirjan mukaan seuraavasti: A) rakentamisen validiteetti: tunnistaa oikeat operatiiviset toimenpiteiden tutkittavat käsitteet; B) sisäinen validiteetti: pyrkii luomaan vapaa tyyli, jossa tietyt edellytykset uskotaan johtavan muihin edellytyksiin, kuten erotettava vääristä suhteista; C) ulkoinen validiteetti: rajataan tutkimuksen aihe, johon tutkimuksen tuloksia voidaan yleistä; D) luotettavuus: osoitetaan toimintaa tutkimuksessa, jossa tietojen keruuprosessi voi liittyä samaan tulokseen. (Patton 2002, 4; Yin 2009, 40; U.S. Goverment Accountability Office 1990; Kidder & Judd 1986, 26–29.)

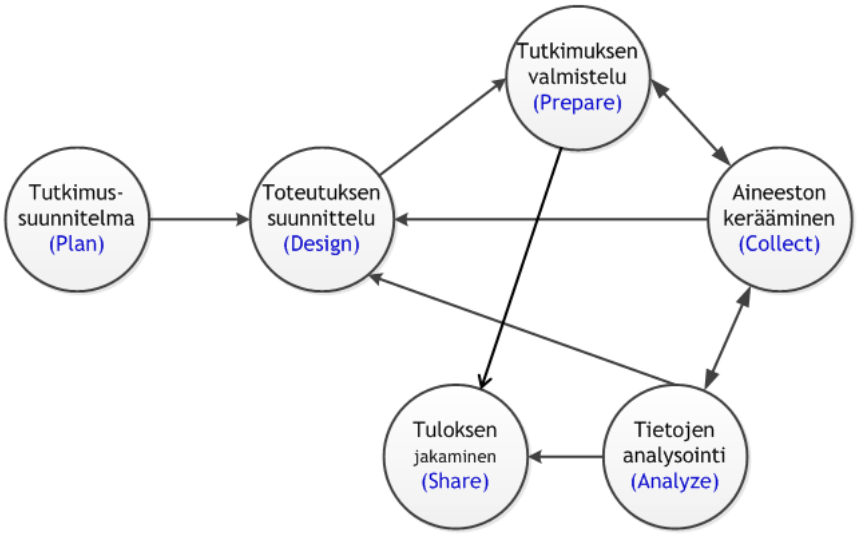
Ensimmäinen askel tapaustutkimuksessa on tunnistaa tutkimuskysymyksiä tai muita perusteita tapaustutkimukselle. Tapaustutkimus auttaa päättämään mitä menetelmää pitäisi käyttää tutkimusprosessissa vertaamalla tapaustutkimuksen etuja ja haittoja muihin menetelmien vahvuuksiin ja rajoituksiin. Tämän tutkimuksen tekemistä varten käytettiin tutkimustapaa, jossa tutkimuskysymyksessä vastataan miten ja miksi- kysymyksiin, taulukko 4. (Yin 2009; Cosmos corporation 1983; Hedrick, Bickman & Rog 1993.)

Menetelmä	(1) Tutkimuskysymyksen muoto	(2) Vaatii tutkijan osallistumista tapahtumiin?	(3) Keskittyminen ajankohtaisiin tapahtumiin
Kokeilu	miten, miksi?	kyllä	kyllä
Tutkimus katsaus	kuka, mitä, missä, kuinka paljon	ei	kyllä
Arkistoanalyysi	kuka, mitä, missä, milloin, kuinka monta, paljonko?	ei	kyllä/ei
Historiatutkimus	miten, miksi, milloin?	kyllä	ei
Tapaustutkimus	miten, miksi?	ei	kyllä

Taulukko 4: Merkityksellisiä tilanteita eri tutkimusmenetelmissä (Yin 2009, 8)

Lainen ym. (2007) mukaan tapaustutkimuksessa tarkastellaan usein monimutkaisia ja pitkään jatkuvia ilmiöitä. Heidän mukaansa tapaustutkimuksen päämääränä on lisätä ymmärrystä tutkittavasta tapahtumasta ja tapahtumaan vaikuttavista olosuhteista. (Lainen ym. 2007, 10.)

Yin:in (2009) mukaan tapaustutkimuksen vaiheet ovat tutkimuskysymykset toteava/ määrittelevä tutkimussuunnitelma (plan). Tutkimusprosessiin sisältyy tutkimuksen toteutuksen suunnittelu (design), tutkimuksen valmistelu (prepare) ja tietojen kerääminen (collect). Tietojen analysointi (analyze) ja jakaminen (share) ovat luonnollisesti osa prosessia. (Yin 2009, 1.) Seuraavassa osiossa on käyty läpi Yin:in 2009 tapaustutkimuksen vaiheet.



Kuvio 7: Tapaustutkimuksen lineaarinen ja iteratiivinen prosessi (Yin 2009, 1)

4.1.2 Toteutuksen suunnittelu (Design)

Tutkimuksen suunnittelun tavoitteena on looginen suunnitelma siitä, miten päästä paikasta A paikkaan B. A:lla tarkoitetaan tässä tapauksessa vastattavaksi esitettäviä kysymyksiä ja B:llä joukkoa johtopäätöksiä, jotka saadaan vastausten perusteella. A:n ja B:n lisäksi voi olla useita merkittäviä vaiheita, kuten esimerkiksi tutkimuskohteen kannalta olennaisen muun tiedon kerääminen ja analysointi sekä vertailu suhteessa kyselytutkimuksessa saatuihin vastauksiin. Kysymysten suunnittelussa on pyrittävä mahdollisimman suureen objektivisuuteen, jotta tulos on mahdollisimman luotettava. Tutkijan on kyettävä kyseenalaistamaan myös omat mahdolliset ennakkoasenteensa ja – odotuksensa. (Yin 2009, 26–27.)

Thomas (2011) korostaa, että tapaustutkimuksen suunnittelussa täytyy pitää mielessä seuraavat asiat: 1) tutkimuksen tarkoitus; 2) tutkimuksen kysymys; 3) kirjallisuus- tai taustaaineiston jäljittäminen ja käyttäminen; 4) päätöksenteon lähestyminen, tutkimussuunnittelun viitekehys, käytettävien menetelmien ja analysointitavan valinta sekä; 5) tutkimusprosessin suunnittelu ja vaiheistaminen. Yin (2009) mitä enemmän tutkimuskysymykset edellyttävät ilmiön tai tutkimuskohteen syvällistä ja kattavaa luotaamista, sitä todennäköisemmin tapaustutkimus on käyttökelpoinen menetelmä. Tapaustutkimuksesta on hyötyä tilanteissa, joissa tutkijalla ei ole lainkaan tai vain vähän mahdollisuuksia vaikuttaa tapahtumien kulkuun. Laine (2007) käytännössä tutkijalla on usein ilmiöistä aiempaa tietämystä ja sen pohjalta hän on

muodostanut alustavan käsityksen tutkimuskohteesta ja siihen liittyvästä problematiikasta. Tutkimusongelman selvittämiseksi tutkija alkaa kehitellä tutkimusta täsmentäviä tutkimuskysymyksiä. Tutkijan täytyy miettiä myös millä keinoin kerätty aineisto auttaa vastaamaan tutkimuskysymyksiin. (Thomas 2011; Yin 2009, 5-14; Laine ym. 2007, 26.)

Järvinen ja Järvinen (2004) viittavat Clark & Causer (1991) tutkimusaiheen valintaan liittyviin kolmeen osaan: (1) alkuperäiset kysymykset, joissa kuvataan mitä halutaan tietää; (2) tutkimuksen perustelu, jossa etsitään vastausta siihen miksi halutaan tietää; ja (3) täsmentävät kysymykset, joiden avulla pyritään etsimään vastausta alkuperäisiin kysymyksiin. Tutkimuksen perusteluja varten voi miettiä, tuottaako tutkimus aidosti uusia löydöksiä tai lisääkö se huomattavasti ymmärrystä aiheesta. (Järvinen ja Järvinen 2004, 5; Clark and Causer 1991.)

4.1.3 Tutkimuksen valmistelu (Prepare)

Yin:in mukaan (2009) tutkimusaineiston huolellinen valmistelu on tärkeää, jotta tutkimus ja tutkimustulosten pätevyys ei vaarannu. Silti tutkimuksen yhteydessä esille saattaa tulla lisäksi seikkoja, jotka eivät ole ennakoitavissa. Tällöin tutkija saattaa joutua harkitsemaan alkuperäistä kysymyksenasetteluaan tai täydentämään tutkimusaineistoaan lisäkysymyksillä, uusilla vastaajaryhmillä tai vertailemalla tutkimustuloksiaan muihin vastaaviin tausta-aineistoihin. (Yin 2009, 67–69.)

Yin (2009) korostaa, että hyvä kysymyssarja muodostaa kokonaisuuden, jossa on selvä jatkumo tai ”juoni”, siten että kysymysten ja vastausten välillä on loogisia mahdollisesti aiemman vastauksen huomioonottavia siirtymiä. Tutkijan on pystyttävä olemaan puolueeton ja ennakkoasenteeton ”kuuntelija”. Toisaalta hänellä on oltava käsitys kysymysten ja vastausten asiayhteydestä sekä käytettävä yksiselitteistä, vastaajien tuntemaa ja ymmärrettävissä olevaa terminologiaa. Tutkijan pitää myös osata tulkita tietoa ja pystyä huomaamaan eri tietolähteiden mahdolliset ristiriitaisuudet. (Yin 2009, 70–72.)

4.1.4 Aineiston kerääminen (Collect)

Yin:in (2009) mukaan jokaisessa tapaustutkimuksen tekemisessä on tärkeä päättää mitä tietojenkeruumenetelmään ensisijaisesti käyttää. Tapaustutkimuksessa käytettävä aineisto voi olla monista eri lähteistä, kuten asiakirjat, haastattelut, tutkijan havainnot, tutkijan osallistuva havainnointi ja havainnot valitsevasta todellisuudesta tai asioiden ilmentymisestä reaalimaailmassa. Tutkimuksen onnistumisen kannalta on tärkeää, että tausta-aineistolähteitä on useita. Liian suppea lähdemateriaalin käyttö voi johtaa yksipuoliseen ja virheelliseen tulokseen. (Yin 2009, 98–99.)

Tutkimusaineiston ja -tulosten olisi oltava myös muidenkin kuin itse tutkijan käytettävissä ja todennettavissa. Mahdollisuuksien ja aineiston luonteen huomioon ottaen tutkimusaineisto

kootaan tietovarastoksi, joka on myöhemmin muiden tutkijoiden käytettävissä, tarkastettavissa, arvioitavissa tai jatkotyöstettävissä. (Yin 2009, 120.)

4.1.5 Tietojen analysointi (Analyze)

Viime vuosien aikana tietotekniset aineistojen analysointityökalut ovat kehittyneet. Niiden avulla laajoja tutkimusaineistoja on mahdollista luokitella aiempaa helpommin. Analyysiohjelmisto on analysointiominaisuuksiensa lisäksi avustava ja luotettava työkalu. Silti loppujen lopuksi tutkija on työkalujen käyttäjä, tulosten tulkitsija ja johtopäätösten tekijä. (Yin 2009, 126–130.)

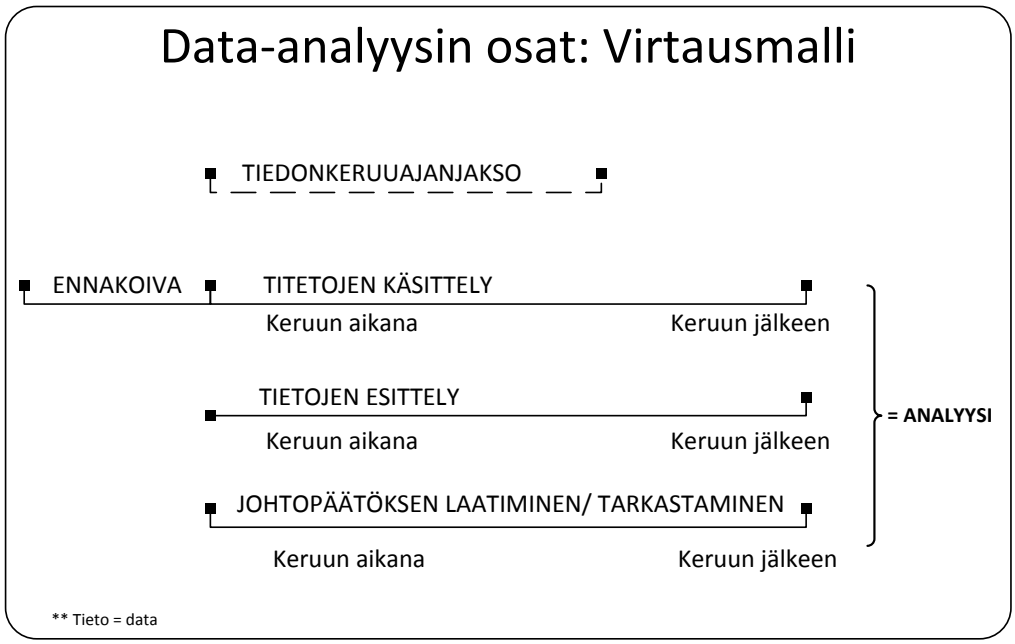
Yin:in (2009) mukaan mitään analyyttisiä tekniikoita ei pitäisi olettaa helppokäyttöisiksi. Kaikki tekniikat edellyttävät paljon harjoitusta käytöstä, jotta niitä voidaan hyödyntää mahdollisimman tehokkaasti. Tutkijan tavoite voisi alkaa vaatimattomasta tutustumisesta, analyyttisten tekniikoiden läpikäynnistä ja omakohtaisesta tärkeimpien tekniikoiden havainnoinnista ja siten rakentaa oma analyyttisten tekniikkojen kokoelma ajan kuluessa. Riippumatta siitä, mitkä tietyt analyyttiset strategiat tai tekniikat on valittu, tutkijan täytyy tehdä kaikkensa varmistaakseen analyysin laadukkuus. Analysoinnissa tutkijan tulee osoittaa, että siinä on huomioitu kaikki aineistot. Keskeisessä asemassa olevat tutkimuskysymykset pitää käsitellä kattavasti lähes tyhjentävän tarkalla tasolla. Tällöin tulkinnoissa ei saa olla ratkaisemattomia yksityiskohtia. Jos tulkinnoissa on aukkoja, analyysi saattaa olla haavoittuva vaihtoehtoisille tulkinnoille, jotka perustuvat tutkimuksessa sivutettuun tai tutkimuksen ulkopuolelle jääneeseen aineistoon. Mikäli mahdollista analyysissa pitäisi keskittyä siihen, että kaikki merkittävät kilpailevat tulkinnat on käyty läpi varsinkin tapaustutkimuksen merkittävimpien näkökohtien osalta. (Yin 2009, 136–161.)

Miles & Huberman (1994) kuvailevat hyvin kerätyn laadullisen datan tärkeyttä, että haastattelemalla tehty datan keräys on merkittävämpää, kuin postin tai puhelimen välityksellä kerätyt datat. Laadullisen datan toinen piirre on niiden rikkaus, paljastavan monimutkaisuuden vahvan mahdollisuuden. Sellaisessa datassa on kattavaa kuvausta ja eläväisyyttä, sisäkkäisyyttä todellisessa kontekstissa sekä se kuulostaa totuudelta, jolla on vahva vaikutus lukijaan. Laadullinen data, joka kerätty samoista aiheista on hyödyllinen, kun tarvitaan valaistusta tai tulkintaa uudelleen. (Miles & Huberman 1994, 10–50.)

Miles & Huberman (1994) nostavat esille sen, että jotkut laadulliset tutkijat pistivät ensisijaisesti tiedonkeruuseen paljon aikaa ja sitten vetäytyvät pois käydäkseen nämä muistiinpanot läpi. Se lannistaa oleellisen koostamista, jotka kyseenalaistavat tutkijan rutiinimaiset oletamukset ja ennakkoasenteet. Miles & Huberman (1994) vahvasti suositellevat varhaisessa vaiheessa analyysiä. Se auttaa tutkijaan punnitsemaan olemassa olevan datan koordinoimista ja analyysia strategioiden kehittämisessä, jolla kerätään uusi ja parempi data. Miles & Huber-

man (1994) pohtivat analyysinongelman kuvaamista, että aina pitää olla tarve pitää taukoa ja miettiä mikä oli tutkimuksen pääkäsite, teemat, asiat ja kysymykset, sekä mitä tutkija näkee tutkimuksen aikana? Ilman sellaista pohdiskelua, on helppoa eksyä suuressa joukossa yksityiskohtiin. (Miles & Huberman 1994, 50.)

Miles & Huberman (1994) kiteyttävät datan analyysin virtausmallit siten (kuvio 8), että laatuanalyysi koostuu kolmesta samanaikaisesta virtaustoiminnosta: tiedon käsittely, tietojen esittely sekä johtopäätöksen laatiminen ja tarkastus. Data- analyysin virtausmallissa tietojenkäsittely viittaa valintaprosessivaiheen datan yksinkertaistamiseen ja muuntamista siten, että muistiinpanoissa tai erimuodoissa olevat tiedot näkyvät tiedekirjalliseen tyyliin. Tämä vaihe tapahtuu jatkuvasti läpi koko laadullisen data-analyysiin elinkaaren sekä ennen tietojen keräämistä. Data-analyysin toinen merkittävä virtaus on datan esittely. Datan esittely on organisoitu, tiivistetty tietojen kokoonpano, joka mahdollistaa päättelemään johtopäätöksen laadinnan ja tarkastuksen. Kolmas virtausmallin analyysin toiminta on johtopäätöksen laatiminen ja todentaminen. Tiedonkeruun alusta alkaen, tutkijan on päätettävä mitkä asiat ovat merkityksellisiä, ettei sisältö ole epäilemättä puutteellinen. Lopulliset johtopäätökset eivät saa ilmestyä ennen kuin tiedonkeruu on ohi, riippuen muistiinpanojen kieliaineiston koosta; koodauksesta-, tallennuksesta - ja käytetyistä hakumenetelmistä ja tutkijoiden ja rahoittajan laadun tarkentamisen vaatimuksesta. Usein tulokset ovat ennustettu alusta alkaen, jopa silloin kun tutkija väittää jatkaneensa päättelyä, joka rakentaa arvion yleisiin ehdotuksiin. (Miles & Huberman 1994, 10–11; Tesch 1982; Faust 1982; Strauss 1987.)



Kuvio 8: Laadullisen analyysin kokonaiskuvaa mukailen (Miles & Huberman 1994, 10)

Johtopäätökset tarkistetaan myös tutkijan toimesta. Tarkastus voi olla tutkijan kirjoittaessa ilmestynyt lyhyt katoavainen ajatus, tai se saattaa olla pohdinnassa ilmestynyt ajatus muiden tutkijoiden tai tutorin kesken, tai kun laajasti pyritään jäljittelemään havaintoa tai löydöstä toista tietokokonaisuudesta. Datan merkityksen ilmaantuminen täytyy testata uskottavasti ja se pitää olla ajan tasalla. Muuten johtopäätöksestä jää mielenkiintoisia tarinoita, että mitä on tapahtunut tuntemattomasta totuudesta ja hyödystä. (Miles & Huberman 1994, 11.)

4.1.6 Tuloksen jakaminen (Share)

Tapaustutkimusraportti ei seuraa mitään stereotyyppistä muotoa, kuten aikakauslehtiartikkeli. Menestynyt tutkija tulkitsee aineistokeruuvaiheen mahdollisuudeksi saada merkittävää kokemusta tai harjoittelua. Oivaltava tutkija alkaa muodostaa tapaustutkimusraporttia jopa ennen kuin tiedonkeruu ja analyysi ovat valmiita. Tapaustutkimuksilla on potentiaalisempaa yleisöä, kuin muun tyyppisillä tutkimuksilla. Kokonaistapaustutkimusraportin suunnittelemisessa tutkimustulosten esittämisessä olennaista on tunnistaa kenelle tutkimusraportti on suunnattu. Eritasoisia kohderyhmiä voi olla useita (asiantuntijat, kyselyyn vastanneet, organisaation johto, muut tutkimuksen tekijät) eikä yksi ja sama tutkimusraportti sovellu välttämättä kaikille kohderyhmille. (Yin 2009, 165–167.)

4.2 Suunnittelutieteellinen tutkimusmetodologia

Tässä luvussa tutustutaan järjestelmän suunnittelutieteellisen tutkimusmetodologian taustoihin, minkälaisia ratkaisuja markkinoilla on saatavilla sekä millaisia kehittämismahdollisuuksia on. Monitahoisia ja -mutkaisia ilmiöitä ja ongelmia tutkittaessa keskeistä on tieteellisten menetelmien objektiivinen soveltaminen osana tutkimusprosessia. (Nunamaker ja muut 1991, 92.)

Järvinen & Järvinen (2004) viittavat Van Aken (2004) mukaan suunnittelutieteen tarkoitus on joko luoda tietämystä järjestelmän suunnittelua ja toteutusta varten muun muassa rakenteellisten ongelmien ratkaisua varten tai nykyisten systeemien suorituskyvyn parantamiseksi. Van Akenin (2004) mielestä uuden innovaation hyödyllisyys on arvioitava ennemmin tai myöhemmin käytännössä. Suunnittelutietämys käsittelee suunnitteluprosessia kolmesta näkökulmasta: innovaation kohteen, järjestelmän toteutuksen ja sen prosessin suunnittelun. Suunnittelutieteessä tutkimuskohde on muuttuva. Suunnittelutieteen teknologinen sääntö määritellään yleisen tietämyksen tihentymäksi, joka liittää intervention tai artefaktin haluttuun tulokseen tai suorituskykyyn sitä valittuun kohteeseen sovellettaessa. (Järvinen & Järvinen 2004, 103; Van Aken 2004.)

Järvinen & Järvinen (2004) viittavat Van Aken (2004) suunnittelutieteen kuvaamisessa korostavan sekä konstruktion että parantamisen käyttävän samanlaista lähestymistapaa ja tuottavan samanlaisen tuloksen, jota kutsutaan teknologiseksi säännöksi. March ja Smithiin (1995) ja Hevner ja muut (2004) painottavat suunnitteluprosessin tarkastelussaan vain konstruointia. Heidän mukaansa suunnittelutieteen tutkimusten tulokset ovat neljän tyyppisiä: käsitteistöjä, malleja, metodeja ja realisointejen toteutuksia. He määrittelevät ne seuraavasti: 1) käsitteistö (constructs) muodostaa tutkimusaiheen sanaston; 2) malli on joukko ehdotuksia, esityksiä tai lauseita, jotka ilmaisevat käsitteiden välisiä suhteita; 3) metodi on joukko askelia (algoritmi tai ohjeisto), joita käytetään tehtävän suorittamiseksi sekä; 4) realisointi (instantiation) on artefaktin toteutus tietojärjestelmänympäristössään. (Järvinen & Järvinen 2004, 103; Van Aken 2004; March ja Smithiin 1995; Hevner ja muut 2004.)

Artefaktien toteutukset ovat käytännön ilmentymiä, toimintamalleja, toimintoja March ja Smith (1995) mukaan käsitteistöjä, malleja ja metodeja. Tavoitetilan kuvaus on itse asiassa malli tilasta, jossa toivomme asioiden olevan, kun olemme toteuttaneet ideamme. Toteuttamisprosessin osana on metodi, jonka avulla uskomme saavamme aikaan muutoksen lähtötilasta tavoitetilaan. Suunnittelutieteellisen tutkimuksen lopputulos on Hevnerin & muiden (2004) mielestä artefakti itsessään. Artefaktin tulee tarjota ratkaisu tutkimusongelmaan ja sen tulisi antaa uutta tutkimustietoa aihealueeseen uudella ja innovatiivisella tavalla. (March & Smith 1995; Järvinen & Järvinen 2004, 103–107; Hevner ja muut 2004, 75–105.)

Hevner & Chatterjee (2010) vahvistavat sen, että perusoletus suunnittelutieteen tutkimuksessa on se, että tieto, ongelman ja sen ratkaisun ymmärtämiseksi suunnittelun rakentamisessa sovelletaan artefaktia. Simon (1996) tulkitsee sen, että termiä artefakti käytetään kuvaamaan jotain, joka on rakennettu ihmisen toimesta, mikä on innovatiivinen, eikä jotain, joka esiintyy luonnossa. (Hevner & Chatterjee 2010; Simon 1996.)

4.3 Järjestelmän kehittämisprosessin vaiheet

Nunamakerin ja muiden (1991) mukaan järjestelmien kehitysprosessin vaiheet ovat ryhmiteltävissä: järjestelmän tarvekartoitukseen (käsitteistön viitekehyksen muodostaminen), määrittelyyn (järjestelmäarkkitehtuurin luominen tai kehittäminen), tarjolla olevien ratkaisujen analysointiin ja valitsemiseen, prototyypin suunnitteluun ja rakentamiseen sekä järjestelmän testauksen ja sen toimivuuden arviointiin, kuvio 9. (Nunamaker ja muut 1991, 96; Ackoff, Gupta & Minas 1962; Arden 1980; Bailey 1982; Basili, Selby, & Hutchens 1986; Benbasat 1984; Blake 1978; Blalock & Blalock 1982.)

4.3.1 Tarvekartoitus

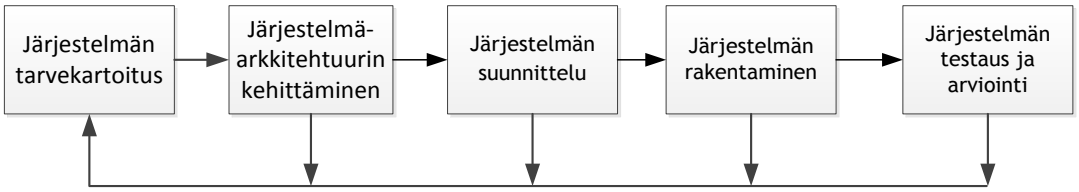
Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) hyväksymä Julkisen hallinno suosituksen (JHS) mukaan tietojärjestelmää kehittäessä eräs tärkeä asia on tulevan järjestelmän tarvekartoitus. Järjestelmän tarve pitää kartoittaa organisaatiossa olevista erilaisista sidosryhmistä. Sidosryhmien tarve voi perustua heidän työnsä parantamiseen, viranomaisen asettaman lain velvollisuuden täyttämiseen tai organisaation strategian asettamaan tarpeeseen järjestelmien kehittämisestä. Tarvekartoitusselvityksen yhteydessä syntyy nykytilan ja tavoitetilan prosessikuvaukset, joilla tulee olla riittävä pohja vaatimusten määrittelyn aloittamiseksi. Näitä asiakirjoja voidaan käyttää lähtötietoina uuden hankittavan järjestelmän määrittelylle. Tarvekartoitusvaiheessa saatuja tietoja pitää täsmentää sekä suunnitella miten viedään läpi vaatimusmäärittely ennen varsinaisen määrittelytyön aloittamista. Järjestelmän vaatimusmäärittelyn tuottamisessa tarkastellaan tarvekartoituksessa saatujen tarpeiden tietoja ja täsmennetään sekä priorisoidaan ne. Vaatimusten määrittely suoritetaan projektina, johon osallistuvat projektin vetäjä, organisaation järjestelmän omistaja, prosessin omistajat ja asiantuntijat sekä tietohallinnon ja tarvittaessa ulkopuoliset asiantuntijat. Ennen vaatimusten määrittelyn hyväksyntää, se viedään asianomaiselle sidosryhmille, asiakkaille ja ulkopuolisille konsulteille katselmoitavaksi. Katselmoinnissa esille tulevat mahdolliset virheelliset määritykset pitää korjata. Vaatimusten määrittelyn korjauksen jälkeen pitää saada hyväksyntä ja lupa aloittaa hanke. (JHS- 173, 2012.)

Tutkijan on hahmoteltava ja perusteltava järjestelmän tutkimuksen kohde ja tarkoitus ennen kuin ryhtyy miettimään yksityiskohtaisempaa tutkimuskysymysten asettelua. Ihanteellinen tutkimuskohde on tutkimusalueelle uusi ja tärkeä. Siihen liittyy innovaatiomahdollisuuksia ja ratkaisemattomia ongelmia. Tutkimuksen kuluessa saatetaan todeta voitavan toimia uudella, aiempaa paremmalla tavalla. Tutkimuskohteen ongelman ratkaisua ei välttämättä voida todistaa käytettävissä/ olemassa olevin matemaattisin tai empiirisin menetelmin. Tuolloin tutkijat voivat halutessaan kehittää järjestelmän osoittamaan ratkaisun pätevyyden esimerkiksi ehdottamalla uusia menetelmiä, tekniikoita tai suunnittelumetodologiaa. Tätä lähestymistapaa kutsutaan todistamiseksi demonstroimalla (proof-by-demonstration). Kun ratkaisu on toteutettu käytännössä, tutkijat voivat havainnoida sen suorituskykyä ja ilmiöitä, jotka liittyvät sen käyttöön, saadakseen tietoa ratkaisun toimivuudesta ja mahdollisesti lisätietoa tutkimuskohteesta. (Nunamaker ja muut 1991, 98–99; Dijkstra 1968; Scott Morton 1984; Halstead 1977; Booch 1986.)

4.3.2 Arkkitehtuurin kehittäminen

Järjestelmäarkkitehtuuri antaa tiekartan järjestelmän kehittämisprosessille. Järjestelmäarkkitehtuurissa määritellään järjestelmän toiminnot sekä komponentit, komponenttien merkitys

järjestelmäkokonaisuuden kannalta sekä komponenttien rajapinnat ja komponenttien välinen vuorovaikutus. Järjestelmän tai toiminnon kehittämistä tutkittaessa on tunnistettava ympäristön asettamat rajoitteet, kehitystyön tavoitteiden tila, kehitystutkimuksen painopiste, sidokset muihin järjestelmiin tai toimintoihin sekä määriteltävän järjestelmälle asetettujen tulostavoitteiden saavuttamiseen vaikuttavat seikat. Järjestelmälle asetettavat vaatimukset on määriteltävä etukäteen niin, että ne ovat mitattavissa ja niiden toteutuminen voidaan vahvistaa toteutettua järjestelmää arvioitaessa suhteessa asetettuihin tavoitteisiin ja vaatimuksiin. Kehittämistutkimuksessa tutkijat eivät yleensä muotoile selkeitä tutkimusolettamia, mutta he tekevät järjestelmän vaatimuksiin liittyviä oletuksia tutkimuksen alalta ja järjestelmän teknisen ympäristön kehittämisestä. (Nunamaker ja muut 1991, 99.)



Kuvio 9: Järjestelmän kehittämisen tutkimusprosessi (mukaillen Nunamaker ja muut 1991, 98)

4.3.3 Suunnittelu

Järjestelmän suunnittelu on eräs tärkeimmistä osa-alueista tietotekniikan hyväksikäyttöön perustuvassa järjestelmän kehitysprosessissa. Suunnitteluprosessiin perustana on käsitys suunnittelun kohteena olevasta osa-alueesta, suunnittelussa sovellettavasta olennaisimmasta tieteellisestä ja teknisestä tietämyksestä, käytettävissä olevista ratkaisuvaihtoehdoista sekä ratkaisuvaihtoehtojen yhdistelymahdollisuudet. Järjestelmän tutkimussuunnittelussa tulisi hyödyntää käytettävissä olevaa teoreettista tietämystä, käsitemaailmaa ja hyväksi havaittuja suunnittelumalleja sekä -menetelmiä. Käytettävissä olevien teknisten tietojen perusteella tulisi luoda kuva/ suunnitelma (blueprint) järjestelmästä ja sen toteuttamisesta. Kehitysjärjestelmän suunnitteluvaiheessa pitää määritellä tietorakenteiden suunnittelu, tietokantoja tai tietämystietokantoja. Lisäksi järjestelmän moduulit ja toiminnot on myös syytä täsmentää samassa vaiheessa sen jälkeen, kun jotain vaihtoehtoa on ehdotettu ja tutkittu sekä lopulliset suunnitelmapäätökset on tehty. (Nunamaker ja muut 1991, 99–100; Denning 1989.)

4.3.4 Rakentaminen

Järjestelmäkehityksen osana on prototyypin luominen. Prototyypin tarkoituksena on varmistaa, että suunnitteluratkaisu vastaa tarvemäärittelyä ja järjestelmälle asetettuja vaatimuksia. Prototyyppi antaa mahdollisesti myös käyttäjäorganisaatiolle mahdollisuuden todeta

konkreettisesti ratkaisun toimivuuden ja mahdolliset kehittämistarpeet. Prototyyppi mahdollistaa järjestelmän testauksen reaalimaailmassa ja sitä kautta on mahdollisesti osa järjestelmän tuotantoon siirtoon. (Nunamaker ja muut 1991, 99–100; Scott Morton 1984.)

4.3.5 Testaus ja arviointi

Nunamakerin ja muiden (1991) viittavat, että järjestelmän rakentamisen jälkeen testaajat voivat testata sen suorituskykyä ja käytettävyyttä. Lisäksi he tutkivat sen vaikutuksia yksittäisen käyttäjän, käyttäjäryhmien tai koko organisaation tasolla. Testitulosten perusteella on arvioitava, että järjestelmätoteutus vastaa järjestelmän määrittelyä ja sille asetettuja vaatimuksia. (Nunamaker ja muut 1991, 100; Basili 1986; Curtis 1985; Ledgard 1987; Mahmood 1987; Orlikowski 1988.)

Pohjoinen (2012) korostaa, täydellisen kattava testauksen paljastavan järjestelmän virheet ja puutteet. Hän kuitenkin toteaa, että kattavan testauksen toteuttaminen on mahdotonta, koska järjestelmän testaukseen vaikuttavia tekijöitä on liikaa. Hyvällä testauksella pystytään toteamaan vain virheiden olemassaolo, ei niiden täydellistä puuttumista. Pohjoisen mukaan testaus jaetaan *moduulitestaukseen*, jossa etsitään vikoja yksittäisistä moduuleista, *integrointitestaukseen*, jossa testataan moduulien yhteistoimintaa sekä *järjestelmätestaukseen*, jossa varmistetaan koko järjestelmän toiminnat ja suorituskyky. (Pohjoinen 2012, 36.)

Arviointi hyödyntää monia samoja metodologioita, joita käytetään perinteisessä sosiaalisessa tutkimuksessa. Kun arviointi tapahtuu poliittisen ja organisatorisen kontekstin sisällä, se vaatii ryhmätaitoja, hallintokykyä, poliittista kätevyyttä, huomaavaisuutta useita osakkaita kohtaan ja muita taitoja, jossa sosiaaliseen tutkimukseen ei yleensä luoteta yhtä paljon. (Donnelly & Trochim 2006.)

Robson & Lindqvistin (2001) mukaan korkealaatuinen arviointi vaati hyvin harkittua tutkimusasetelmaa ja havaintoaineiston keräämistä, analyysiä ja tulkintaa. He toteavat tutkimuksen ja arvioinnin eroavaisuudesta, että arviointi pitää sisällään ajatuksen arvon määrittämisestä. Tutkimus puolestaan koskee toisenlaisia toimintoja, kuten kuvaamista, selittämistä ja ymmärrystä. (Robson & Lindqvist 2001, 25.)

5 Tutkimuksen toteutus

Tässä luvussa käsitellään tutkimuksen konkreettinen toteutus.

5.1 Tutkimuskyselyn suunnittelu

Tutkimuksessa käytettävien tutkimuskysymyksien laatimiseksi taustamateriaalina oli sisäinen tarkastusraportti. Sen perusteella valmistelin tutkimuskyselyn ja lähetin sen organisaation esimiehille. Kaupungin sisäiseltä tarkastustoimelta sain luvan käyttää tietojärjestelmien käyttäjähallintaa koskevaa tarkastusraporttia taustamateriaalina (liite 5). Tutkimuskyselyn esimiehille lähettäminen oli ainoa vaihtoehto, joka mahdollisti vastausten saamisen tutkimuskysymyksiin. Ghauri & Grønhaug (2005) kirjoittavat laadullisesta tutkimuksesta sen, että kvalitatiivista tutkimusmenetelmä korostaa ymmärtämään ilmiöiden vastaajien näkökulmasta. Vastaajalle kysymykset eivät suoraan kertoneet, että tarkoitus oli selvittää esimiesten käsitystä tietojärjestelmien käyttöoikeuksien hakuprosessista ja käyttöoikeuksien sisällöstä. Sen sijaan kyselyssä korostettiin vastaajan kokemuksen merkitystä prosessin kehittämisessä, palautteen saamisen tärkeyttä ja kyselyn tulosten vaikutusta organisaation tuleviin tietojärjestelmäkehityshankkeisiin. Tämän tutkimuksen ja esityksen tekijän näkemyksen mukaan vastaukset kuvasivat esimiesten todellisia mielipiteitä sekä annettu palaute oli suoraa ja aitoa (liite 1 tutkimuskysymykset). (Ghauri & Grønhaug 2005, 108–109.)

Tutkimuskysymykset lähetettiin 182 esimiehelle, joista 64 esimiestä vastasi kyselyyn. Kysymysten vastausaika oli 7.11.2011 – 11.11.2011. Muistutuksena kysymyslinkki lähetettiin uudelleen 9.11.2011. Vastausprosentille ei ollut asetettu vastaajamäärätavoitetta. Tutkimuksen vastausprosentti vaikuttaa pienehköltä. Vastausajankohdan ja esimiesten työtilanteeseen nähden 35 % vastausprosenttia voi kuitenkin pitää tyydyttävänä vastausten analysoimiseksi ja tulosten relevanttiuden kannalta. Vastaustulokset oli jokaisen kysymyksen osalta esitettävissä Webropol- ohjelmiston avulla graafisena esityksenä.

5.2 Kyselyn rakenne

Varsinaiset tutkimuskysymykset on ryhmitelty neljään osaan: esimiesten tausta, käyttäjätunnus- ja käyttöoikeushakuprosessi, käytössä oleva käyttöoikeushakulomake ja käyttöoikeuksien sisältö. Kysymyksien vastaajat on luokiteltu organisaation toimialan, esimiehen työkokemuksen ja esimiehen alaisten määrän mukaan. Kyselyn alussa oli saatekirje, joka kertoi syyn kyselyyn, sen tavoitteen ja vastausten merkityksen kyselykohteen kehittämisessä. Kyselyyn vastaaminen oli vapaaehtoista ja anonyymiä. Kysymyksiä oli 27, joista kaksi kysymystä oli vapaamuotoisesti vastattavia ja yksi oli ei-pakollinen kysymys. Lukuun ottamatta edellä mainittua kolmea kysymystä, muut kysymykset eivät olleet ohitettavissa vastaamatta. Osa kysymyk-

sistä oli väittämiä, joihin vastaaja saattoi vastauksellaan ottaa kantaa. Seitsemässä tutkimuskysymyksessä oli myös ”En osaa sanoa”- vastausvaihtoehto. Tämän vaihtoehdon perusteella oli tarkoitus arvioida esimiesten tietämystä mm. käyttöoikeushakuprosessista ja hakulomakkeesta sekä sitä, onko heitä pystytty tiedottamaan riittävästi asiasta.

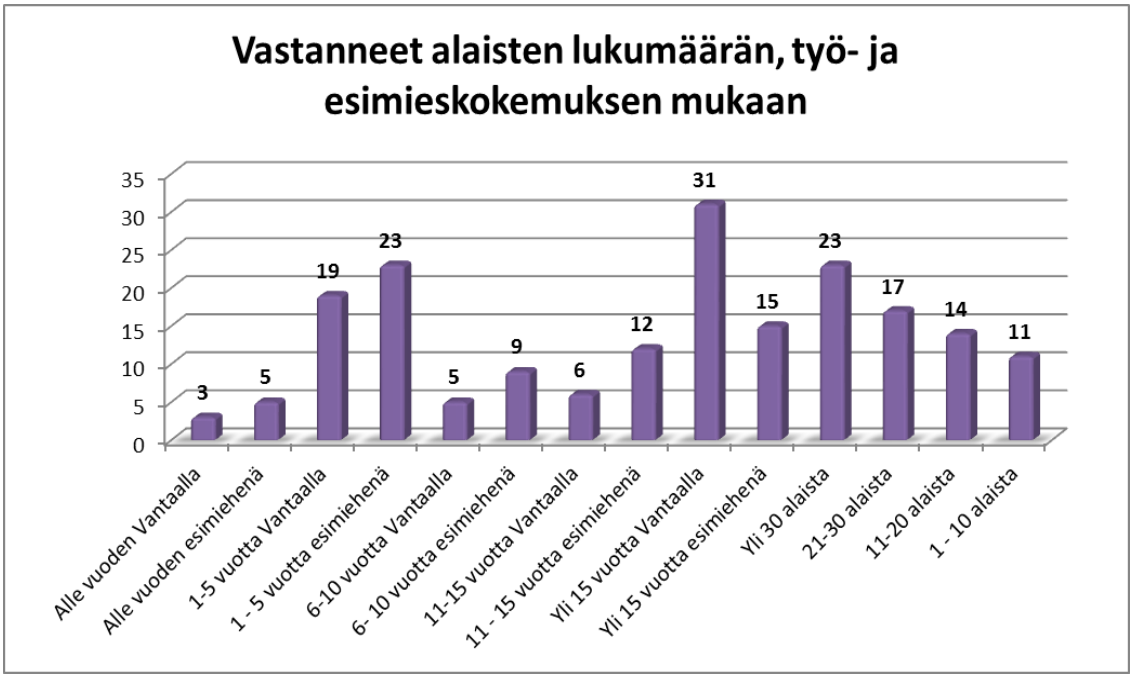
Kyselyn lisäksi haastateltiin organisaation kolmen merkittävän järjestelmän pääkäyttäjää sosiaali- ja terveystoimesta, sivistystoimesta ja keskushallinnon toimialalta. Pääkäyttäjä vastaa tietyn järjestelmän pääkäyttäjätehtävistä ja tietyissä tapauksessa tarkistaa esimiehen hyväksymät käyttöoikeuspyynnöt, etteivät esimiehet hyväksy liian laajoja käyttöoikeuksia. Yleensä esimiehet ovat yhteydessä pääkäyttäjään käyttöoikeuksien sisällön selvittämiseksi. Näistä syistä päädyin haastattelemaan kolmea pääkäyttäjää. Pääkäyttäjän haastattelussa kävimme läpi 15 kysymystä ja haastattelut kestivät noin 20 min (liite 2). Nämä kysymykset ovat pääpiirteeltään jaettu kahteen ryhmään. Yhdeksän kysymystä käsittelee pääkäyttäjän ylläpitämän järjestelmän käyttöoikeushakuprosessia. Kuusi kysymystä käsittelee puolestaan pääkäyttäjän kokemusta esimiehen käyttöoikeushakuprosessin käsityksestä. Pääkäyttäjien haastattelun tarkoitus oli saada ymmärrystä siitä, miten esimiehet ymmärtävät käyttöoikeushallintaprosessia pääkäyttäjien näkökulmasta sekä saada selville miten pääkäyttäjien ylläpitämien järjestelmien käyttäjätunnus- ja käyttöoikeushallinta on hoidettu.

Pääkäyttäjille esittämäni kysymykset ovat valtionhallinnon tietoturvallisuuden osa-alueiden arvioinnissa käytettävän, tietojärjestelmien käyttöturvallisuuden osa-alueita käsittelevästä kysymysluettelosta. Kysymykset koskivat roolien käyttöä järjestelmissä, käyttöoikeushallintaa, vaarallisia työyhdistelmiä ja käyttöoikeuksien käsittelyä. (Haastattelukysymykset ovat liitteessä 2).

5.3 Kyselyn ryhmittely

Esimiehille esitetyn kyselyn alussa oli kolme kysymystä, joilla kartoitettiin vastaajan taustaa. Tätä tietoa käytettiin vastausten ryhmittelyssä. Ryhmittelyn perusteena olivat toimiala, esimiehen alaisten määrä ja työkokemus vuosina esimiestehtävissä. Toimialaryhmittelyllä oli arvioitavissa millä toimialalla vastausten perusteella vaikutti olevan erityisen haastava tilanne, tiedon puutetta tai väärinkäsityksiä käyttöoikeushakuprosessista ja sen sisällöstä. Toimialoja oli yhdeksän kappaletta, joista yhden toimialan osalta ei saatu vastauksia eli ei löydetty vastaajakandidaatteja. Esimiesten alaisten määrä- ryhmittelyllä pyrittiin selvittämään onko alaisten määrällä ja välillisesti alaisten määrästä aiheutuvalla käyttöoikeuskäsittelytilanteiden määrällä vaikutusta esimiehen käsitykseen ja tietoon käyttöoikeushakuprosessista ja siinä käsiteltävästä tiedosta. Alaisten määrä- vastausvaihtoehdot olivat 1-10, 11–20, 21–30 tai yli 30 alaista. Esimiesten työvuodet esimiestehtävissä- kysymyksellä pyrittiin selvittämään miten työkokemus vaikuttaa käyttöoikeushakuprosessia ja sen sisältöä koskevaan tietämykseen.

Esimiestehtävän työkokemus vastausvaihtoehdot olivat 1 -5, 6-10, 11–15 tai yli 15- vuotta. Tutkimuksessa käytettiin analysointiyksikkönä esimiesten käyttäjähallintaprosessin tuntemusta. Analyysin tulos jaettiin toimialaan, työkokemukseen sekä alaisten määrään. (Kuvio 10).



Kuvio 10: Tutkimuskyselyn vastanneiden tausta

6 Tulokset ja analysointi

6.1 Esimiesten kyselyn analysointi

Tämän tutkimuksen kysely on tehty kyselytutkimusten tekemiseen ja analysointiin soveltuvalla Webropol–ohjelmalla, jota on mahdollista käyttää Internet-selaimella. Vastaajakandidaateille toimitettiin sähköpostitse kyselyyn vastaamiseen kannustava saateviesti ja kysymyslinkki. Tutkimuskysymysten suunnittelun ja laadinnan yhteydessä yhtenä näkökulmana tekijällä oli miten vastaukset ovat analysoitavissa. Tutkimuksen analysointia varten on hyödynnetty sisäisen tarkastuksen toimenpide-ehdotuksia ja VAHTI- käyttövaltuushallinnon periaatteita ja hyviä käytännön suosituksia. Näiden pohjalta tutkimuksessa analysoitiin tietämyksen tasoa organisaatiossa esitettyjen kysymysten osalta. Vastausten analysoinnissa käytettiin organisaation toimialaryhmittelyä ja seuraavia näkökulmia: 1) tietoturvan huomioonottaminen; 2) tietämys alaisten käyttöoikeuksista ja niiden merkityksestä; 3) esimiesvastuu käyttöoikeuksien osalta sekä; 4) käyttöoikeuksienhaku ja –hyväksyntäprosessi.

Alustavan analyysin perusteella vastauksia ryhmiteltiin ja kysymysten merkitystä painotettiin kysymyksien tärkeyden kannalta. Yhdistelmäraportin tuottamiseksi vastauksista käytettiin myös mm. Microsoft Excel-ohjelmistoa.

Kyselyyn vastanneista suurin osa oli Sosiaali- ja terveystoimesta 41 % sekä Sivistystoimesta 20 %, mikä on luonnollista, koska Sosiaali- ja terveystoimiala ja Sivistystoimiala ovat työntekijämäärältään suurimpia toimialoja. Lisäksi toimialoilla on runsaasti työntekijöiden vaihtuvuutta ja esimiehet joutuvat usein hakemaan käyttäjätunnuksia ja käyttöoikeuksia. Keskushallinnon toimialan vastaajien määrä oli 13 %. Noin 48 %:lla kysymyksiin vastanneista oli yli 15 vuoden esimieskokemus. Vastaajista 30 %:lla oli 1 – 5 vuotta kokemusta esimiestehtävistä.

6.1.1 Tutkimuskysymyksien ymmärrettävyys

Tutkimuskysymyksissä kysyttiin ”Tiedätkö millainen käyttäjätunnus- ja käyttöoikeushakuprosessi organisaatiolla on käytössä?”. Noin 80 % vastasi ”Kyllä” ja 20 % vastasi ”En”. Lisäksi kysyttiin myös ”Kuka voi hakea tai myöntää tietojärjestelmien käyttäjätunnuksia ja käyttöoikeudet?”. Kaikista vastaajista 86 % vastasi esimiehen voivan hakea ja 6 % vastasi pääkäyttäjän. 50 % vastaajista oli sitä mieltä, että tietojärjestelmien käyttäjätunnukset ja käyttöoikeudet hyväksyy Tietohallinnon palvelukeskus. Sen sijaan 20 % vastasi pääkäyttäjä, 6 % vastasi oma esimies, 5 % vastasi minä itse ja 16 % en osaa sanoa. (Kuvio 11.) Todellisuudessa organisaatiossa esimiehellä on oikeus hakea sekä hyväksyä käyttäjätunnukset ja käyttöoikeudet.

Kuvio 11. Kuka voi myöntää käyttöoikeudet

6.1.2 Esimiesten tietämys alaisten tarvitsemista käyttöoikeuksista

Yhteensä 72 % vastaajista oli sitä mieltä, että he tietävät mitkä käyttöoikeudet heidän alaisillaan pitää olla kussakin tietojärjestelmässä. Toisaalta 28 % vastaajista ei tiennyt. (Kuvio 12.)

Kuvio 12. Alaisilla olevien käyttöoikeuksien tuntemus

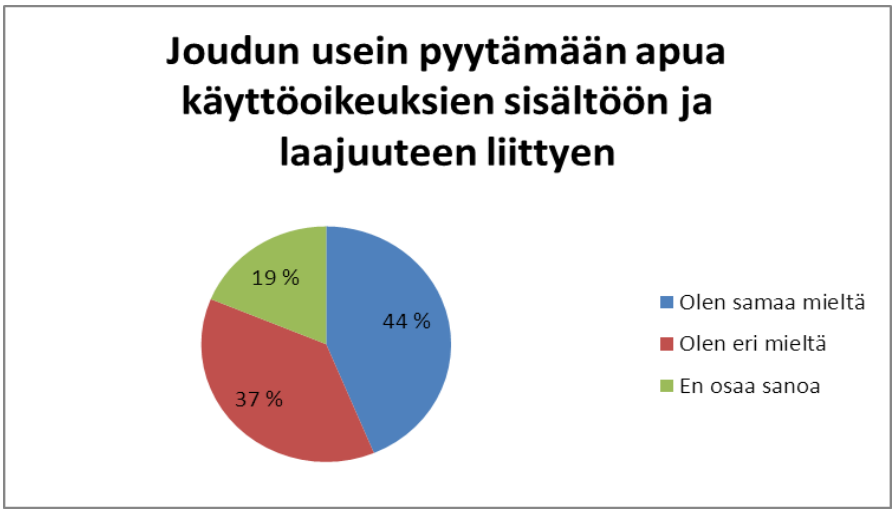
Kyselyssä kysyttiin myös miten esimies saa tiedon alaisiensa tarvitsemista käyttöoikeuksista. Yli puolet ilmoitti itse tietävänsä alaistensa tarvitsemat käyttöoikeudet kussakin järjestelmässä. Noin 15 % vastaajista on saanut tiedon toimistosihteeriltä, soittamalla kollegalleen tai omalta esimieheltään. Muut ovat saaneet tiedon pääkäyttäjältä, HelpDeskiltä tai alainen itse

on selvittänyt tarvitsemansa käyttöoikeudet ja esittänyt ne esimiehelleen haettavaksi. (Kuvio 13.)

Kuvio 13. Miten esimiehet selvittävät alaisiensa tarvitsemat käyttöoikeudet

6.1.3 Käyttöoikeuksien sisältö ja laajuuden ymmärtäminen

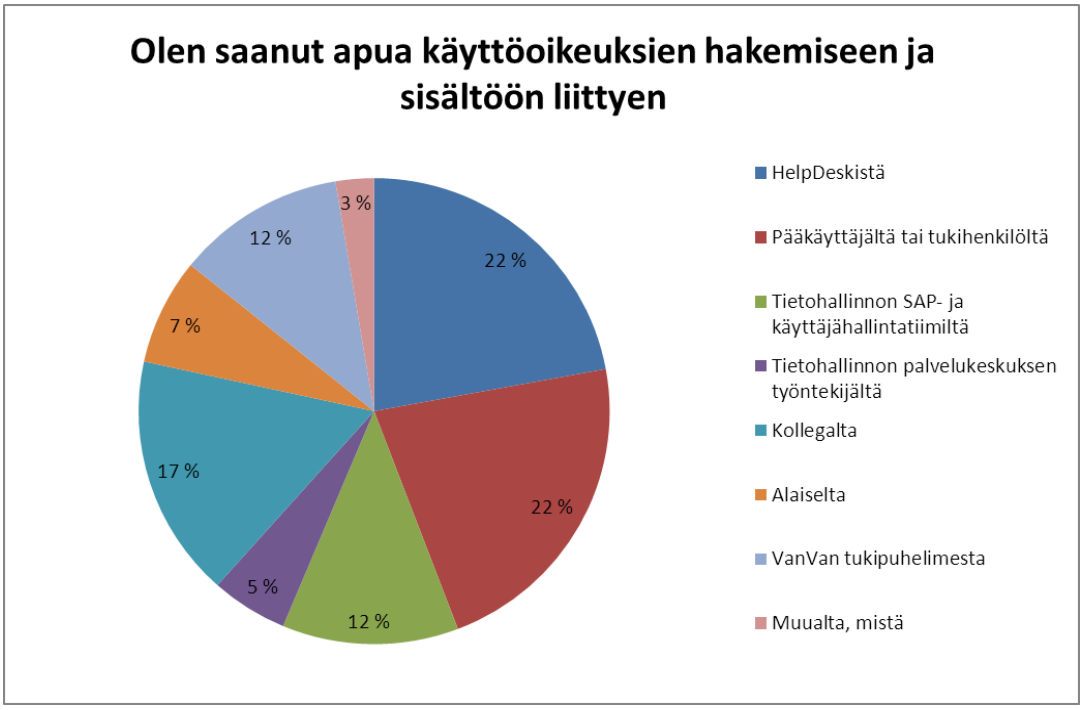
Noin puolet vastaajista oli sitä mieltä, että he joutuvat usein pyytämään apua käyttöoikeuksien sisältöön ja laajuuteen liittyen. (Kuvio 14.)



Kuvio 14. Mitä mieltä esimiehet ovat avunpyytämisestä käyttöoikeuksien laajuuteen

Kysyttiin mistä esimiehet saavat apua käyttöoikeuksien hakemiseen ja sisällön selvittämiseen. Kysymysten vastausvaihtoehdoissa oli mahdollisuus valita enemmän kuin yksi vastaus. Suurin

osaa vastaajista on saanut apua 22 % HelpDeskistä ja 22 % pääkäyttäjiltä tai tukihenkilöiltä. 5 % on saanut apua Tietohallinnon henkilöstöltä, 15 % Tietohallinnon SAP- ja käyttäjätiimiltä, ja 12 % kollegalta, 7 % alaiselta, 17 % VanVan (Vantaan toiminnanohjausjärjestelmä) tukipuhelimesta ja loput 3 % jostain muualta. (Kuvio 15.)



Kuvio 15. Mistä esimiehet saavat apua käyttöoikeuksien hakemiseen ja sisältöön

Tutkimuksessa kysyttiin vapaasti vastattavana ”Mitä tietoja tarvitset, jotta pystyt hakemaan käyttöoikeuksia alaisillesi?”. Vastauksia tuli runsaasti kysymykseen liittyvistä eri asioista. Seuraavassa on esimerkkejä vastauksista:

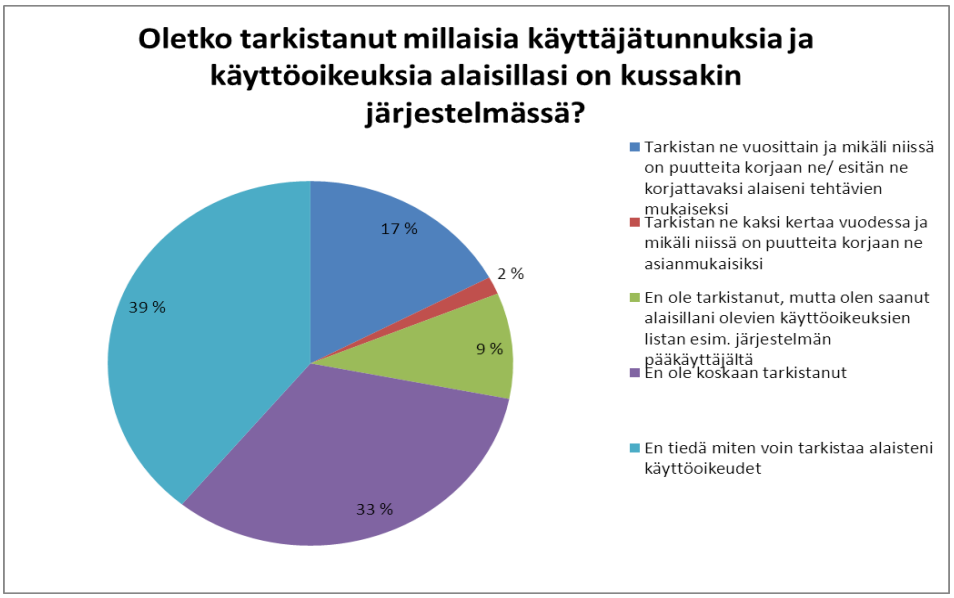
1. Tiedän missä tehtävässä työntekijä tulee työskentelemään. Ja olisi mielenkiintoista tietää, mitkä käyttöoikeudet hänellä on ennestään, jos hän siirtyy alaisekseni kaupungin toisesta yksiköstä
2. Varmaan koulutusta siitä mitä kaikkia oikeuksia on olemassa ja mihin tai kuka niitä tarvitsee. Samoin jonkinlaista listaa tms. siitä mistä niitä haetaan ja miten niitä täytetään. Nyt olen joutunut soittelemaan ympäriinsä ja kyselemään neuvoa
3. käyttöoikeuksien laajuudesta voisi laatia jonkin ohjeistuksen ts. mitä milläkin tasolla.
4. Työtehtävät ja niiden hoitamisessa tarvittavat järjestelmät. Mitä mikäkin kohta sap-käyttäjähakemuksissa tarkoittaa (sap- kokonaisuus on edelleenkin sekava)
5. Henkilötiedot, tehtävätiedot, ja niihin kuuluvat käyttöoikeuksien rajaukset ja käyttöoikeuksien koodit
6. Järjestelmien erilaisien roolien tunteminen, oman organisaatiossa päätetyt työtehtäviin kuuluvat roolit, mistä mitäkin saa ja miten löydän ajan tasalla olevat tiedot.

7. Käyttöoikeudet suhteessa henkilön toimenkuvaan ja vastuisiin
8. Työntekijän tehtävä- ja henkilötiedot
9. Kuinka nopeasti mitäkin tunnukset myönnetään
10. Tarvitsen yhdestä paikasta tiedon, mistä käyttöoikeudet haetaan, kuka voi asiassa auttaa, kuinka laajoja käyttöoikeuksia tulee hakea, mihin järjestelmiin minulla on oikeus hakea käyttöoikeuksia
11. Selkeät listat, mitä kaikkia ohjelmia ja tunnuksia eri työntekijät tarvitsevat, esim. koulusihteeri.

6.1.4 Käyttöoikeusprosessin tuntemus toimialueen mukaan

Kysyttiin: Tunnetko käyttöoikeushakemuksia koskevat Vantaan kaupungin tietoturvaohjeet? Yhteensä 90 % vastaajista tuntee käyttöoikeushakemuksia koskevat organisaation käytössä oleva tietoturvaohjeet. Muut 10 % vastaajista ei tiedä ohjeiden olemassaolosta. Todellisuudessa kaikki käyttäjät ovat sitoutuneet perehtymään tietojärjestelmien käyttäjätunnusten edellytyksenä olevassa, allekirjoittamassaan tietoturvasitoumuksessa tietoturvaohjeisiin ja noudattamaan niitä.

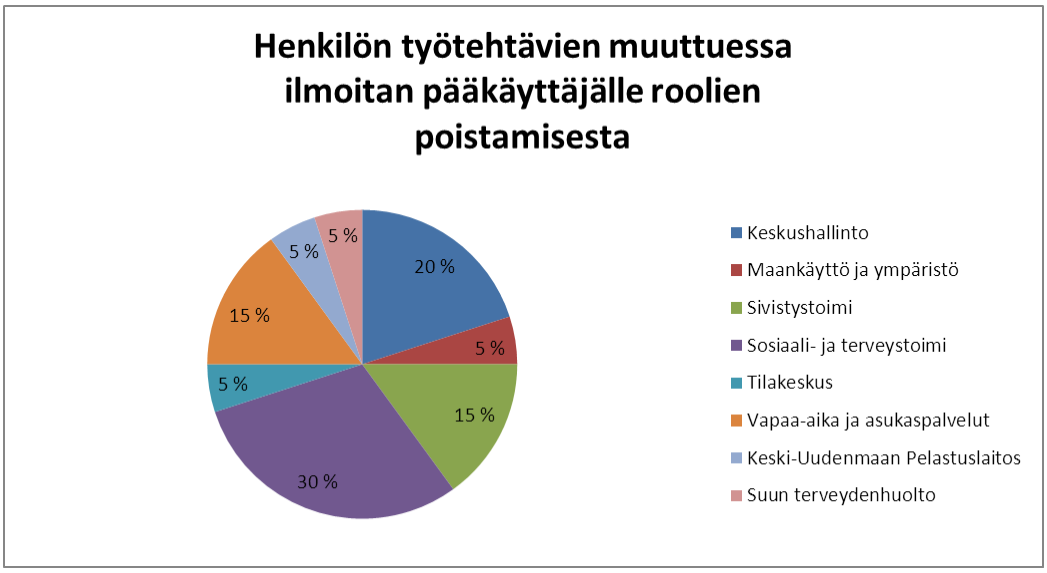
Kysyttiin myös onko esimies tarkistanut millaisia käyttäjätunnuksia ja käyttöoikeuksia hänen alaisillaan on kussakin järjestelmässä. Yli puolet vastaajista ei tiedä miten voi tarkistaa tai ei ole koskaan tarkistanut alaistensa käyttöoikeuksia. (Kuvio 16.) Lisäksi kysyttiin, arvioiko esimies alaisen toimenkuvan muuttuessa alaisen käyttöoikeuksien muutoksen tarpeellisuutta. Noin 70 % on sitä mieltä, että he arvioivat käyttöoikeudet ja ne pidetään ajan tasalla. 25 % vastasi, että muutoksen tarpeellisuus huomataan ja arvioidaan, mutta he eivät tiedä, mitä toimenpiteitä heidän tulee tehdä käyttöoikeuksien ajan tasalla pitämiseksi. 8 % vastaajista oli sitä mieltä, että käyttöoikeuksiin ei kiinnitetä huomiota toimenkuvan muuttuessa. Kuitenkin näissä vastauksissa on mielestäni ristiriitoja.



Kuvio 16. Alaisilla olevien käyttäjätunnuksien ja käyttöoikeuksien tarkistaminen

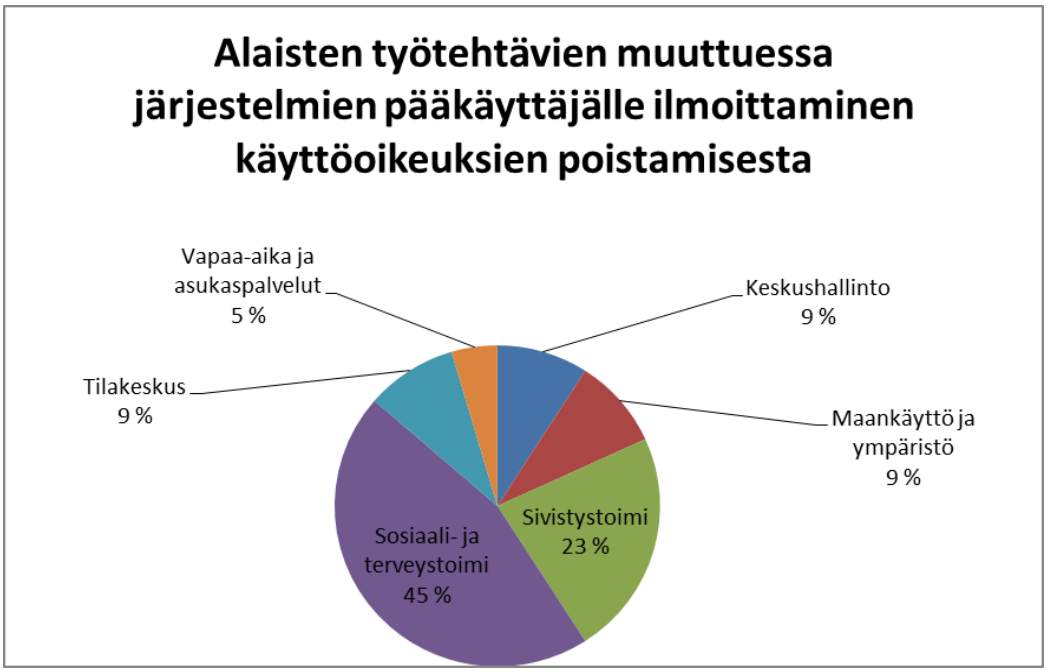
Kysyttiin ilmoittaako esimies järjestelmien pääkäyttäjälle alaisen työtehtävän muuttuessa tai siirttyessä organisaation sisällä toisen työyksikköön tai tehtävään, että käyttöoikeudet tulee poistaa. Yli puolet ilmoittaa alaisen työtehtävien muuttuessa pääkäyttäjille käyttöoikeuksien poistamisesta. Noin 25 % on sitä mieltä, että alaisen työtehtävien muuttuessa he ilmoittavat pääkäyttäjälle, mutta eivät pysty osoittamaan mitkä käyttöoikeudet alaisella on käytössä. Noin 20 % vastasi, etteivät he alaisen työtehtävän muuttuessa ilmoita pääkäyttäjälle tilanteesta lainkaan.

Henkilön työtehtävän muuttuessa ”ilmoitan pääkäyttäjälle roolien poistamisesta”-vaihtoehdon vastanneista oli 30 % sosiaali- ja terveystoimesta, 20 % keskushallinnosta, 15% sekä sivistystoimen, 15 % vapaa-aika ja asukaspalvelusta, 5 % maankäyttö ja ympäristötoimesta, 5 % suun terveydenhuollosta, 5 % Keski- Uudenmaan Pelastuslaitoksen ja 5 % tilakeskuksen kustakin toimialalta. (Kuvio 17.)



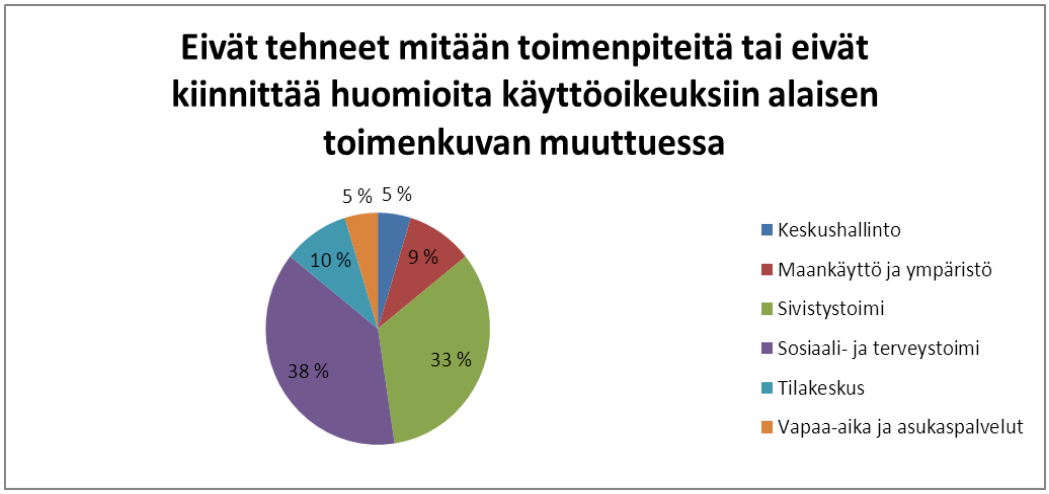
Kuvio 17. Alaisten työtehtävien muuttuessa pääkäyttäjille ilmoittaminen toimialoittain

Koko kyselyn vastaajista 22 % vastasi ”henkilön työtehtävien muuttuessa en ilmoita pääkäyttäjälle” ja 23 % ”ilmoittavat pääkäyttäjälle, mutta eivät pysty osoittamaan mitkä käyttöoikeudet heidän alaisillaan on”. Näistä esimiehistä oli 45 % sosiaali- ja terveystoimesta, 23 % sivistystoimesta, 9 % maankäyttö ja ympäristö, 9 % tilakeskus, 9 % keskushallinnon toimialoilta ja 5% vapaa-aika ja asukaspalvelutoimialalta. (Kuvio 18.)



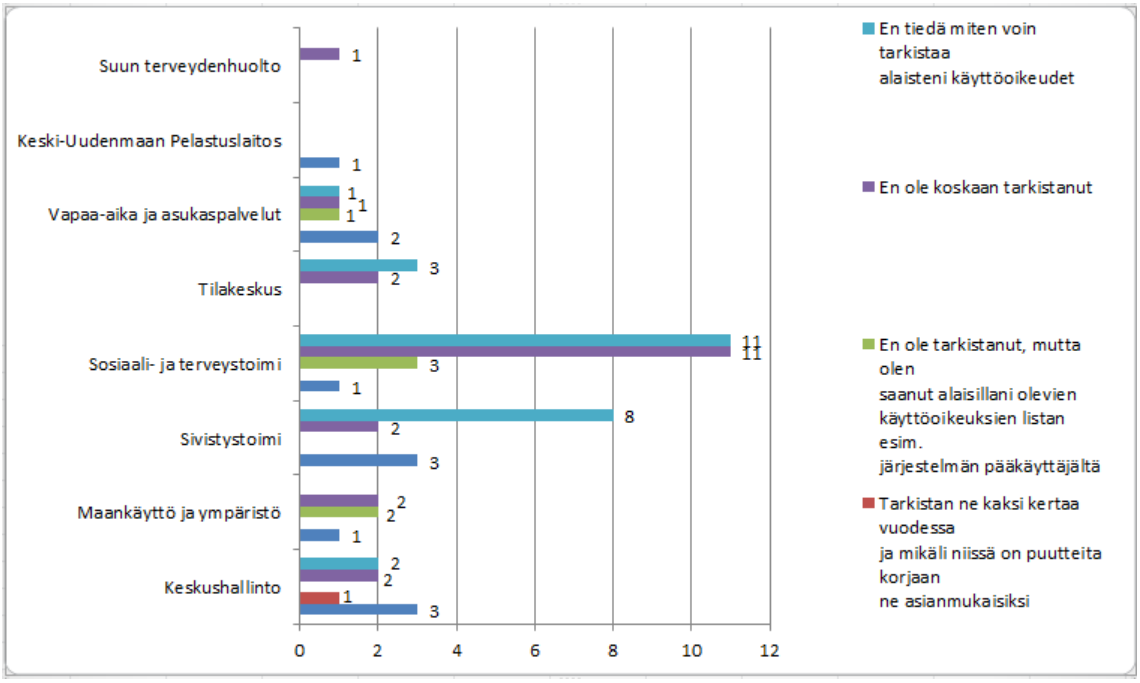
Kuvio 18. Esimiehet, jotka eivät ilmoita pääkäyttäjille alaisten työtehtävien muuttuessa ja jotka ilmoittavat, mutta eivät pysty osoittamaan mitkä käyttäjäroolit hänellä on ollut käytössä toimialoittain

Yhteensä 51 % esimiestä vastasi, että alaisien toimenkuvan muuttuessa alaisten käyttöoikeudet arvioidaan ja ne pidetään ajan tasalla. Muut esimiehet vastasivat, että he huomaavat ja arvioivat muutoksen tarpeellisuuden, mutta eivät tehneet mitään toimenpiteitä tai eivät kiinnittää huomiota alaisen käyttöoikeuksiin toimenkuvan muuttuessa. (Kuvio 19.)



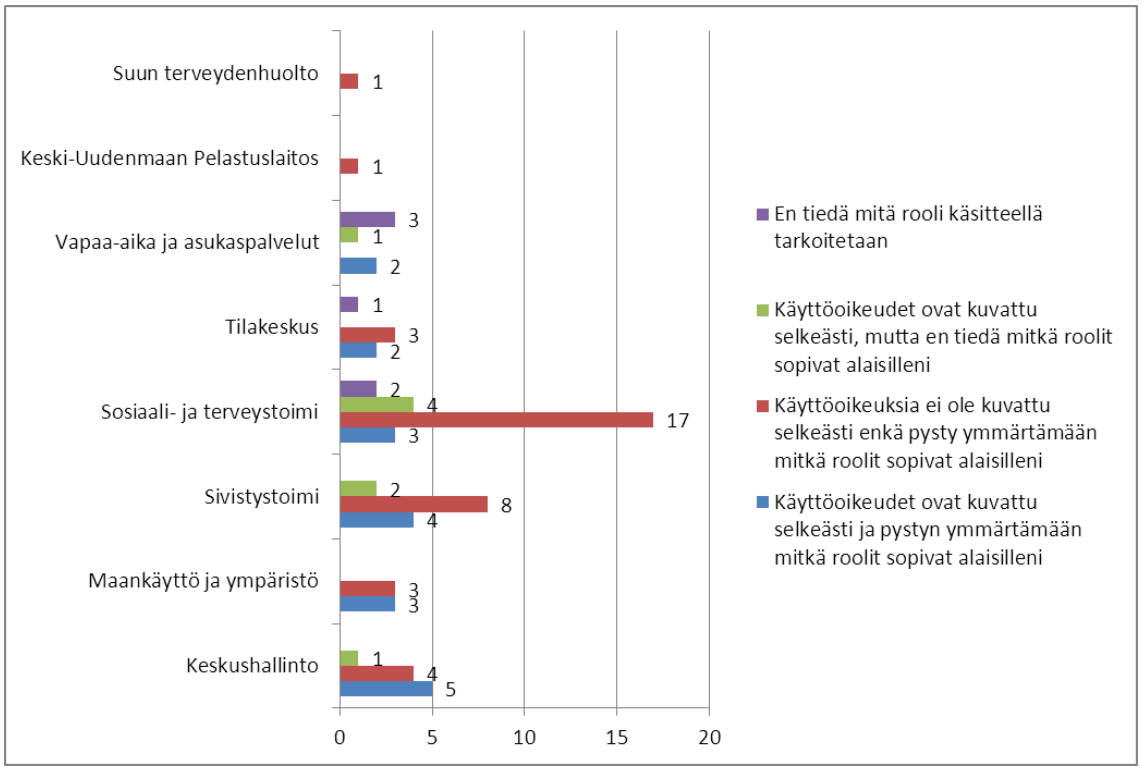
Kuvio 19. Esimiehet, jotka eivät tehneet mitään toimenpiteitä tai kiinnittää huomiota käyttöoikeuksiin alaisen toimenkuvan muuttuessa jaoteltuna toimialoittain

Kysyttiin onko esimies tarkistanut millaisia käyttäjätunnuksia ja käyttöoikeuksia hänen alaisillaan on kussakin järjestelmässä. 39 % ei tiennyt miten he voisivat tarkistaa alaisten käyttöoikeudet, 33 % ei ole koskaan tarkistanut, 19 % tarkistaa ne vuosittain tai kaksi kertaa vuodessa ja mikäli niissä on puutteita korjaa ne tai esittää ne korjattavaksi alaisen tehtävän mukaiseksi. 9 % vastaajista ei ole tarkistanut, mutta he ovat saaneet alaisillaan olevien käyttöoikeuksien listan esim. järjestelmän pääkäyttäjältä. Kuviossa 20 nämä vastaukset on jaettu toimialoittain.



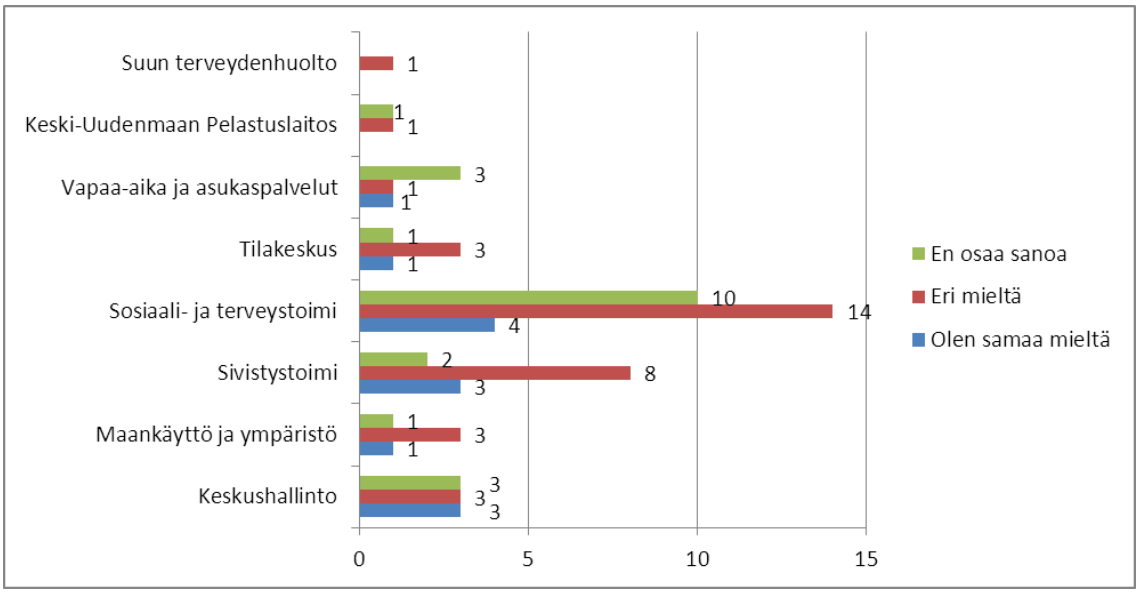
Kuvio 20. Alaisilla olevien käyttöoikeuksien tarkistaminen toimialoittain

Kysyttiin onko esimiehen alaisilleen hakemat käyttöoikeudet kuvattu käyttöoikeuslomakkeella siten, että ne vastaavat alaisten tarkoitettua tarvetta ja toimintavaltuuksia. 53 % on sitä mieltä, että käyttöoikeuksia ei ole kuvattu selkeästi, eikä esimies pystyy ymmärtämään mitkä roolit sopivat hänen alaisillensa. 27 % vastasi, että käyttöoikeudet on kuvattu selkeästi ja he pystyvät ymmärtämään mitkä roolit sopivat heidän alaisilleen. Muut 20 % olivat sitä mieltä, että käyttöoikeudet on kuvattu selkeästi, mutta he eivät tiedä mitkä roolit sopivat heidän alaisilleen tai he eivät tiedä mitä rooli- käsitteellä tarkoitetaan. Kuviossa 21 nämä vastaukset ovat jaettuna toimialoittain.



Kuvio 21. Käyttöoikeuksien kuvauksien ja käsitteistön tuntemus toimialoittain

Lisäksi esitettiin kantaa otettavaksi väite ”käyttöoikeuslomakkeessa olevat kuvaukset käyttöoikeuksista ovat selkeitä”. 50 % oli eri mieltä, 19 % oli sama mieltä ja loput 31 % eivät osanneet sanoa. Nämä tuloksen ovat jaettu toimialoittain kuviossa 22.



Kuvio 22. Esimiesten mielipide käyttöoikeuksien selkeydestä toimialoittain

6.1.5 Käyttöoikeusprosessin tuntemus

Tässä kappalessa kuvataan esimisten käyttöoikeusprosessin tuntemus suhteessa alaisten määrään ja esimiestehtävään. Suurin osa esimiehistä ei tarkista alaistensa käyttöoikeuksia. Kaikista vastaajista 60 % oli esimiehiä, joilla on yli 20 alaista. Heistä puolet ei tiennyt miten he voivat tarkistaa alaisensa käyttöoikeudet ja puolet ei ole koskaan tarkistanut. Kaikki esimiehet, jotka eivät tienneet miten alaisten käyttöoikeudet tarkistetaan tai eivät koskaan niitä tarkistaneet yli 60 %:lla oli 10 vuotta esimieskokemusta. Yksi henkilö, joka on ollut yli 15 vuotta esimiestehtävissä ja jolla on yli 10 alaista, vastasi tarkistavansa alaisten käyttöoikeudet kaksi kertaa vuodessa. Lisäksi mikäli niissä on puutteita, niin hän korjaa ne asianmukaisiksi. Noin 20 % esimiehistä, joilla on alle 5 vuotta esimieskokemusta, ei tiedä miten he voivat tarkistaa alaistensa käyttöoikeudet. Näistä suurimmalla osalla on alle 20 alaista. (Taulukko 5.) Käyttöoikeuksien tarkistamattomuus korostuu niiden esimiehien osalta, joilla on paljon alaisia ja pitkähkö työkokemus.

Esimiesten tausta ja alaisten määrä	Tarkistan ne vuosittain ja jos niissä on puutteita, korjaan tai esitän ne korjattavaksi alaiseni tehtävien mukaiseksi	Tarkistan ne kaksi kertaa vuodessa ja mikäli niissä on puutteita korjaan ne asianmukaisiksi	En ole tarkistanut, mutta olen saanut alaisillani olevien käyttöoikeuksien listan esim. järjestelmän pääkäyttäjältä	En ole koskaan tarkistanut	En tiedä miten voin tarkistaa alaisteni käyttöoikeudet
Esimies kokemusta					
Alle vuoden	1			1	1
1 - 5 vuotta	3		2	4	13
6 - 10 vuotta	4		1	3	1
11 - 15 vuotta	2			4	6
yli 15 vuotta	1	1	3	9	4
Alaisten määrä					
1 - 10 alaista	6			2	3
11 - 20 alaista	3		4	2	4
21 -30 alaista				7	9
Yli 30 alaista	2	1	2	10	9

Taulukko 5. Vastanneiden esimiesten lukumäärä, työkokemus ja alaisten määrä sekä miten he ovat tarkistaneet alaistensa käyttäjätunnuksia ja käyttöoikeuksia kussakin järjestelmässä.

6.1.6 Käyttöoikeushakuprosessin kehittäminen

Tutkija teki tukipalvelupisteelle tulleiden tukipyyntöjen osalta taustatutkimusta. Tukipalvelupisteelle tuli tammi – syyskuun 2012 aikana noin 30600 kappaletta työpyyntöä ja keskimäärin kuukausittain noin 3400 tukipyyntöä. Taustatutkimuksen mukaan käyttäjätunnuksiin ja käyttöoikeuksiin liittyvien tukipyyntöjen osuus oli 39 %. Eli käyttäjätunnuksiin ja käyttöoikeuksiin liittyvien tukipyyntöjen määrä kuukausittain on 1340 kpl (taulukko 6). Tutkijan mielestä tämä on merkittävä määrä.

Ongelman tyyppi	**Määrä**	**%**	**Kuukaudessa kpl**
CHANGE REQUEST	7025	23 %	781
CANNOT ACCESS	12063	39 %	1340
HARDWARE PROBLEM	1671	5 %	186
SOFTWARE PROBLEM	3034	10 %	337
WASTE	1707	6 %	190
HOW TO	3773	12 %	419
CANNOT PRINT	955	3 %	106
OPERATE	367	1 %	41
Yhteensä	**30595**	**100 %**	**3399**

Taulukko 6: Vantaan tukipalvelupisteelle tulleiden tukipyyntöjen määrä tammi - syyskuun 2012 aikana

Tutkimustuloksen analysoinnin alkuvaiheessa huomasin, että kyselyyn vastanneista suurin osa oli Sosiaali- ja terveystoimesta ja Sivistystoimesta. Analysointivaiheen edettäessä kiinnitin huomiota näillä molemmilla toimialoilla olevan merkittävän työntekijöiden vaihtuvuushaasteen. Tämän tiedon varmistamiseksi sekä arvioidakseni kuinka esimiehet joutuvat hakemaan käyttäjätunnuksia ja käyttöoikeuksia, tein taustatutkimuksen yhteenvedon organisaatiossa tehdyistä uusien ja poistuneiden tunnuksien määrästä toimialoittain. Taustatutkimus on tehty tammikuun 2011 – syyskuun 2012 ajan tapahtumista (taulukko: 7). Tämä taustatutkimus osoitti, että Sivistystoimessa ja Sosiaali- ja terveystoimessa on tehty ja poistettu eniten tunnuksia. Näin ollen kyselytutkimuksen tulos antoi todellisuutta vastaavan kuvan.

Toimialat	Työntekijöiden määrä	Uudet tunnukset	Uusi keskimäärin kuukaudessa	Poistuneet Tunnukset	Poistuneet keskimäärin kuukaudessa
Sosiaali- ja terveydenhuolto	3192	1081	105	1406	156
Sivistystoimi	5596	1263	123	1895	181
Keskushallinto	390	122	12	160	15
Maankäyttö ja Ympäristö	748	159	15	300	28
Suun terveydenhuolto	320	77	9	104	12
Tilakeskus	1066	220	21	435	40
Vantaan Työterveys	71	39	47	42	5
Vapaa-aika ja Asukaspalvelut	914	479	5	646	59
Keski-Uudenmaan Pelastuslaitos	500	77	8	72	9
Yhteensä	12797	3517	345	5060	505

Taulukko 7: Organisaation työntekijöiden vaihtuvuus toimialoittain 01/2011- 09/2012

Nykyisessä käyttöoikeushakuprosessissa tunnukset ja käyttöoikeudet haetaan eri menetelmillä mm. itsepalveluportaali, -pdf, MS-Word- lomake ja sähköpostiviestillä. Tutkimuskyselyssä kysyttiin, että ”Miten kehittäisit käyttäjätunnus- ja käyttöoikeuksienhakuprosessia?”. Kysymys oli vapaamuotoisesti vastattavissa ja sai esittää kehittämistoiveita. Vastauksia tähän kohtaan saatiin 27 vastaajalta. Vapaamuotoiset vastaukset on analysoitu seuraaviin aiheisiin: 1) nykyprosessitilanne; 2) käyttäjätunnuksen liittyviä asioita sekä; 3) kehitettäviä kohteita.

1) Nykyisestä käyttöoikeuksien hakuprosessista koettiin, että hallittavia järjestelmiä on useita ja tunnuksia haetaan useasta paikasta. Tietoja käsitellään manuaalisesti ja se tuottaa ylimääräistä työtä varsinkin esimiehille, jotka hakevat tunnuksia tai oikeuksia useammalle kuin yhdelle alaiselle. Esimiehet kokivat alaisten tehtävien ja toimenkuvien muuttuvan jatkuvasti ja toisaalta, että esimiehillä ei ole tietoa pysyvätkö oikeudet tilanteen tasalla; 2) Esimiehet kokevat käyttäjätunnuksen saamisen ajoissa liian työlääksi ja monimutkaiseksi. Uudelle esimiehelle tai työntekijälle tarvittavan käyttäjätunnuksen saaminen kestää useita työpäiviä jopa viikkoja. Yksi vastaaja totesi, että tunnuksien ja käyttöoikeuksien selvittämisen menee 3-4 päivää vuositasolla. Esimiehet kokivat hankalana, että kaikki oikeudet ja käyttäjätunnukset

on haettava erikseen. Lisäksi sähköpostiosoitetunnuksien muoto koettiin hankalana henkilöille, jotka käyttävät virallisena nimenään jälkimäistä etunimeään (kutsumanimi). Koettiin, ettei käyttäjätunnusten ja- oikeuksien käsittelyprosessiin voi luottaa täydellisesti. Esimerkiksi esimiehet joutuva selvittämään liian usein, miksi heidän hakemaansa alaisen käyttäjätunnusta ei ole luotu; 3) Kyselynvastaajat kokivat hyvänä ratkaisuna esimiehen nimeämät henkilöt nk. ”tunnuspyytäjät”, jotka pystyvät hakemaan ja koordinoimaan tunnukset ja käyttöoikeuksien anomusta. Suurin osa vastaajista esitti, että he haluaisivat ”Yhden polun”, jossa valitaan mitkä tunnukset ja käyttöoikeudet haetaan. Käyttöoikeutta haettaessa toivottiin saatavan yhteenveto, mitä käyttöoikeuksia haettavilla henkilöllä on. Koettiin myös hyvänä, jos pystytään järjestämään yhteyshenkilö (tietohallinnosta ja jokaiselta toimialalta), johon voi olla yhteydessä heti, kun tunnusten saannissa on ongelma tai niitä on odotettu jo useampi päivä. Lisäksi toivottiin, että käyttöoikeushakujärjestelmän vastuu- ja yhteyshenkilöt voisi ottaa paremmin esille. Toivottiin, että koko käyttöoikeus- ja käyttäjätunnushakuprosessista olisi selkeä, mielellään graafinen kuvaus ja selkokieliset ohjeet. Eräs henkilö kiteytti kehitystoivomuksensa: *”Ymmärrän, että meidän kaikki ohjelmat ja järjestelmät eivät ole saman tahon hallinnoimia. Toivoisin kuitenkin, että pääsisimme siihen tilanteeseen, että meillä on yksi lomake, johon täytetään henkilötiedot ja raksitaan kaikki henkilön tarvitsemat ohjelmat yms. Voisiko tämä näin sähköisenä aikana, jopa toimia niin, että kaikkien ohjelmapyynnöt ohjautuisivat tästä suoraan oikeisiin osoitteisiin”.*

6.1.7 Vaarallisten työyhdistelmien hahmottaminen

Suurin osa esimiehistä ei hahmota, miten syntyy vaarallisia työyhdistelmiä. Se johtuu monestakin syystä. Ennen kaikkea ei ole kuvattu työtehtävien, tietojärjestelmäroolien ja työroolien yhdistelmämäärittelyä. Lisäksi ei ole työkalua, jolla pystyy ennalta estämään vaarallisten työyhdistelmien syntymisen. Vastausten mukaan suurinta osaa haettavissa olevista käyttöoikeuksista ei ole kuvattu selkeästi eivätkä he tiedä mitkä roolit sopivat heidän alaisillensa. Lisäksi henkilön työtehtävän muuttuessa suurin osa esimiehistä ei välttämättä ilmoita pääkäyttäjälle eikä arvioi muutoksen mahdollisesti aiheuttamaan tietoturvariskiä. Yli puolet vastaajista ei tiedä miten voi tarkistaa tai ei ole koskaan tarkistanut alaistensa käyttöoikeuksia. Noin puolet vastaajista pyytää apua käyttöoikeuksien sisällön ja laajuuden ymmärtämiseksi. Eräs selkeä syy vaarallisten työyhdistelmien syntymiselle on se, että käyttöoikeushakulomakkeessa ei ole selkeästi kuvattu käyttöoikeuksien sisältöä ja laajuutta.

6.2 Pääkäyttäjien haastatteluiden analysointi

Pääkäyttäjien haastattelut tehtiin eri ajankohtina. Alussa haastateltiin pelkästään sosiaali- ja terveystoimen edustajaa. Jotta haastattelun otos edustaisi mahdollisimman eri toimialoja sekä tutkimuksen tulos ei toisi vain yksipuolista näkökulmaa, haastateltiin lisäksi kahta muuta

pääkäyttäjää, sivistystoimen ja keskushallinnon toimialalta. Pääkäyttäjähaastattelujen avulla selvitettiin kahta eri näkökulmaa. 1) Ensin tiedusteltiin pääkäyttäjien kokemuksia siitä miten esimiehet käsittävät käyttöoikeuksien käsitteet, käyttöoikeuskäsittelyprosessin ja miten esimiehet vertailevat ja pitävät ajan tasalla alaisiensa käyttöoikeuksia. 2) Toinen näkökulma oli pääkäyttäjien ylläpitämä järjestelmien käyttäjätunnus- ja käyttöoikeuksien hallintaprosessi sekä vaaralliset työyhdistelmät. Pääkäyttäjien haastattelut on purettu ylämainitun näkökulman mukaisesti.

6.2.1 Pääkäyttäjien kokemus

Tässä kappalessa selvitetään pääkäyttäjien kokemus esimiehien käyttöoikeushakuprosessin käsityksestä.

Kysyttiin pääkäyttäjiltä, että ymmärsivätkö esimiehet nykyisen käyttöoikeushakuprosessin ja sen sisällön. Kaikki pääkäyttäjät totesivat, että pääsääntöisesti esimiehet ymmärtävät käyttöoikeusprosessin annon ja tietävät, että käyttöoikeus pitää hakea järjestelmien pääkäyttäjiltä. Yksi haastateltavista oli puolestaan sitä mieltä, etteivät kaikki esimiehet välttämättä tiedä kuinka käyttöoikeushakuprosessi menee. Erään pääkäyttäjän mielestä uusille esimiehille asia pitää aina selittää juurta jaksain. Hän uskoo kuitenkin esimiehien ymmärtävän asian niin, että esimiehet hakevat alaisilleen käyttöoikeudet, joka he työtehtävissään tarvitsevat. Yhden pääkäyttäjän mielestä esimiehille on pyritty myös selittämään mitä on käyttäjätunnus ja mitä kaikkea sillä voi tehdä. Kuitenkin kaikki pääkäyttäjät kokevat, että esimiehet eivät välttämättä ymmärtää mitä käyttöoikeuksien (roolin) sisällä on ja kuinka laajasti käyttäjä pystyy käsittelemään asioita ko. järjestelmässä.

Haastateltavilta kysyttiin, onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu. Kaksi pääkäyttäjää kertoi, että hakuprosessista on tiedotettu eri tilaisuuksissa ja viestintäkanavissa muun muassa sähköpostitse, puhelinkeskusteluissa ja koulutustilaisuuksissa. Näistä kahdesta pääkäyttäjästä yksi totesi, että hänen edustamansa järjestelmän osalta käyttöoikeuksien käsittelystä ja myöntämisestä ei todennäköisesti ole olemassa pysyvää kirjallista ohjetta. Kolmas pääkäyttäjä ei itse tiedä kuinka hyvin muut pääkäyttäjät ovat saaneet erilaista käyttöoikeuskäsittelyprosessi ohjeistusta. Lisäksi hän totesi, ettei hän tiedä sitäkään kuka voisi ohjeistaa uusia esimiehiä, kun edellinen esimies vaihtuu. Onko niin, että itse esimies joutuu kysymään ja hänellä kerrotaan vai miten? Pääkäyttäjän mielestä jatkuvasta ohjeistamisesta ei ole tehty selvää prosessikuvausta. Käytännössä perehdyttäminen on osa uuden työntekijän perehdyttämissuunnitelmaa ja ko. olevan uuden esimiehen.

Jokaiselta pääkäyttäjältä kysyttiin, huolehditaanko tietojen päivittämisestä vastuuhenkilöiden vaihtuessa. Kaksi pääkäyttäjää vastasi, että käyttöoikeuksien ajantasalla pitäminen on haas-

tavaa ja hankaa. Yksi näistä pääkäyttäjistä totesi, että esimiehet huolehtivat asiasta jollain aikavälillä. Hän piti käyttöoikeuksien poistamista ongelmana, koska esimiehet eivät edelleenkään ota pääkäyttäjiin välittömästi tai suoraan yhteyttä muutoksista. Kaksi pääkäyttäjää saa jotain kautta selville, että henkilö on lähtenyt pois kaupungin palveluksesta ja pääkäyttäjät oma-aloitteisesti käyvät läpi ja tarkastavat käyttäjätunnuksien ajantasaisuutta. Toinen näistä pääkäyttäjistä kertoi, että osa esimiehistä huolehtii ilmoituksesta ja osa ei toteutunut ollenkaan. Hän totesi, että hän ei ole nähnyt selkeätä prosessikuvausta siitä miten esimiehet huolehtivat vastuuhenkilötietojen päivittämisestä. Lisäksi hän totesi, että hänen vastuullaan olevassa järjestelmässä on paljon tunnuksia, joita ei ole käytetty useampaan vuoteen, eikä niitä ole passivoitu tai poistettu. Kolmas pääkäyttäjä korosti, että hänen ylläpitämässä järjestelmässä vastuuhenkilöiden vaihtuessa tietojen päivittäminen järjestelmään on tärkeää ja toteutuu nopealla aikataululla. Hän totesi, että työpisteissä asiaa käsitellään kriittisenä, koska järjestelmän tiedetään olevan merkittävä operatiivinen järjestelmä. Esimiesten lisäksi pääkäyttäjä itse huolehtii, että uudella henkilöllä ja hänen sijaisellaan on työssä tarvittavat sopivat käyttöoikeudet, eikä liian laajat oikeudet. Jos uudelle henkilölle tai sijaiselle on haettu liian laajat käyttöoikeudet, pääkäyttäjä puuttuu asiaan ja pitää ne oikealla tasolla.

Pääkäyttäjille esitettiin kysymys, tarkistetaanko roolien ajantasallaolo henkilön toimenkuvan muuttuessa. Yksi pääkäyttäjä totesi, että mikäli työpisteestä tulee ilmoitus, että henkilön työtehtävät ovat muuttuneet, niin he tekevät muutokset. Tieto tulee usein ko. henkilöltä itseltään, hän korosti ”ei yleensä koskaan esimiehiltä”. Toinen pääkäyttäjä vakuutti, että hänen vastuullaan olevassa järjestelmässä on pakko saada tieto välittömästi esimieheltä työtehtävän muuttuessa. Hän koki myös saavansa tiedon käytännössä viiveettä. Kolmas pääkäyttäjä totesi, että henkilön työsuhteen muuttuessa pääkäyttäjät tarkastavat henkilön käyttöoikeudet.

Pääkäyttäjiltä kysyttiin myös, tekeekö tietojärjestelmän pääkäyttäjä asiallisen tarkastuksen ennen käyttöoikeuden myöntämistä. Eräs pääkäyttäjä totesi, että käyttöoikeudet myönnetään esimiehen hakemuksen mukaisesti. Yleensä pääkäyttäjät tietävät mitkä käyttöoikeudet kenellekin pitää olla. Hän kuitenkin huomautti, että mahdollisesti olisi tarpeen käydä nykyistä tarkemminkin läpi sitä, mitä käyttäjä tekee ja minkälaisia oikeuksia hänelle annetaan. Toisaalta hänen mielestä henkilön työsuhteen alussa ei ole välttämättä vielä selvillä mitä kaikkea hänen tehtäviinsä kuuluu tai mitä tehtäviin kuuluvista asioista hän konkreettisesti hoitaa. Toinen pääkäyttäjä vakuutti, että hänelle tulee esimiehen tarkistamalomake, jossa on työntekijän tiedot, ja allekirjoitetut sitoumukset. Hän korosti, että esimiehellä on vastuu siitä, että hän tarkistaa esimerkiksi työntekijän henkilöllisyyden viranomaisten antaman henkilötodistuksesta. Kolmas pääkäyttäjä totesi, että he tarkastelevat kriittisesti käyttöoikeuspyyntöjä. Mikäli pyynnössä on jotain epäselvää tai puutteita, pääkäyttäjä puuttuu asiaan.

6.2.2 Pääkäyttäjien ylläpitämät järjestelmät

Seuraavasti selvitettiin pääkäyttäjien ylläpitämien järjestelmien käyttäjätunnus- ja käyttöoikeushallinta kokemusta.

Pääsääntöisesti kaikki pääkäyttäjät ilmoittivat, että heillä ei ole systemaattista suunnitelmaa esimiesten ohjeistamisesta. He totesivat, että uusille esimiehelle ja myös muillekin asiasta on kerrottu eri foorumeissa tai yhteydenotoissa. Erään pääkäyttäjän mukaan ohjeistusprosessi pitäisi kuvata selkeästi, jotta esimiehillä on ajantasainen tieto käyttöoikeuksien käsittelyprosessista.

Pääkäyttäjiltä kysyttiin, onko työrooliin liittyvät oikeudet kuvattu riittävän tarkasti. Yksi pääkäyttäjistä mainitsi, että käyttöoikeudet ovat muokattu ajan myötä lain ja lakimuutosten vaatimusten mukaisesti. Pääkäyttäjä totesi, että käyttöoikeudet on toteutettu ammattinimikkeen pohjalta lainsäädännön asettamat vaatimukset huomioonottaen. Toinen pääkäyttäjä totesi, että ko. järjestelmän pääkäyttäjät (työryhmä) keskenään käyvät läpi, että mitä käyttöoikeuksia pitää olla kenelläkin. Hänen vastaamaansa järjestelmää kehitetään kokoajan ja käyttöoikeudet on kuvattu tarkasti, mutta työ on kesken ja ne ovat päivittämättä ja tällä hetkellä dokumentointi on puutteellista. Hän totesi, että järjestelmästä saa tulostettuna käytössä olevat käyttäjätunnukset ja käyttöoikeudet. Kolmas pääkäyttäjä totesi puolestaan, että yhden hänen tiimikollegansa toimesta käyttöoikeudet on ylläpidetty ja kuvattu hyvin. Aikaisemmin käyttöoikeudet eivät ole kuvattu hyvin ja erityisesti kolmen viime vuoden aikana on panostettu käyttöoikeuksien kuvauksien ajantasallesaattamiseen. Jos uusia käyttöoikeuksia tarvitaan tai olemassa olevasta jotain puuttuu, pääkäyttäjät yhdessä järjestelmän toimittajan kanssa miettivät ja toteuttavat sen.

Haastattelussa kysyttiin onko käyttöoikeushallinta integroitu henkilöstörekisterin/ HR-järjestelmän kanssa. Kaikkien pääkäyttäjien vastuulla olevat järjestelmät eivät ole integroitu henkilöstörekisterin kanssa. Yksi pääkäyttäjistä totesi, että hänen vastuullaan olevan järjestelmän ja henkilöstöjärjestelmän integraatio on ollut esillä. Haastatteluiden perusteella tietojärjestelmin käyttäjätunnuksia ei tällä hetkellä verrata henkilöstöjärjestelmään.

Kysyttiin myös kuinka usein käyttöoikeus- ja henkilörekisterien tietoja verrataan. Pääkäyttäjät vastasivat, että kaikkia heidän ylläpitämiä järjestelmiä ei verrata henkilörekisterin kanssa. Haastattelussa kysyttiin, verrataanko vastuuhenkilötietoja henkilörekisteriin. Kaikki pääkäyttäjät vastasivat, että pääsääntöisesti vastuuhenkilötietoja ei verrata henkilörekisteriin eikä väestörekisteriin. Yksi pääkäyttäjä huomautti, että ”*näin tietysti tulisi varmaan toimia, mutta varmasti siitä en voi sanoa, että näin toimittaisiin*”. Hän kuvasi haastatteluhetken tilannetta, että esimies palkatessaan pyytää työntekijän todistukset ja varmentaa, että henki-

löllä on oikeat paperit ja oikeudet. Sen lisäksi esimiehen on syytä täydentää kaikki tiedot käyttäjätunnuksia pyydettäessä. Eräs pääkäyttäjä totesi, että jos uutta tunnusta tehtäessä tulee jotain epäselvää tai puutteellisilla tiedoilla esitettyä, niin pääkäyttäjä tarkistaa henkilöstörekisterissä asian manuaalisesti. Hän kuitenkin kaipaa, että hänen ylläpitämä ja henkilöstörekisterin yhdistäminen tuo lisäarvoa heidän työlleen. Toisen pääkäyttäjän mielestä esimiehen tekemään käyttäjätunnushakemukseen on voitava luottaa. Siitä huolimatta hän totesi tarkistavansa, että työntekijä, jota hakemus koskee, on allekirjoittanut käyttäjätunnusten saamisen edellytyksenä olevan tietoturvasitoumuksen.

Haastattelussa kysyttiin, onko käyttöoikeuksien hallinta keskitetty. Kahden pääkäyttäjän ylläpitämien järjestelmien käyttöoikeudet hallitaan itse järjestelmässä kunkin pääkäyttäjän toimesta. Eräs pääkäyttäjä haastattelun aikana kuvasi tilannetta, että tällä hetkellä käyttöoikeushallinta ei ole keskitetty yhteen paikkaan. Kaikki esimiehet voivat hakea jossain toimitepisteissä. Jossain toimipisteessä voi olla joku muu nimetty henkilö, joka käsittelee käyttöoikeuksia. Hän totesi, että ”*kukaan ei varsinaisesti varmaan tiedä kuinka monessa paikassa niitä on*”.

Kysyttiin myös sulkeutuvatko käyttöoikeuksiin liittyvät käyttäjätunnukset automaattisesti tietojen muuttuessa henkilöstörekisterissä. Kaikki kolme pääkäyttäjät totesivat, että käyttöoikeuksien liittyvät käyttäjätunnukset ei sulkeudu automaattisesti. Eräs pääkäyttäjä totesi, että suurin osa tunnuksista suljetaan pääkäyttäjän oman aloitteen perusteella. Esimieheltä tulee ilmoitus harvoin. Toisen pääkäyttäjän ylläpitämässä järjestelmässäkin kaikki tunnukset sulkeutuvat manuaalisesti. Kolmas pääkäyttäjä korosti, että käyttöoikeudet on ehdottomasti pyydettävä poistamaan tai muuttamaan, kun käyttäjän työsuhteen päättyessä tai työtehtävän muuttuessa. Pääkäyttäjät tekevät järjestelmästä raportin ja, jos käyttäjätunnusta ei ole käytetty, niin he poistavat sen.

Kysyttiin pääkäyttäjiltä onko työntekijällä rajattu pääsy vain omiin työtehtäviinsä liittyviin tietoihin. Kaikkien pääkäyttäjien ylläpitämissä järjestelmissä on pääperiaate, että työntekijällä on pääsy järjestelmään hänelle annettujen käyttöoikeuksien rajauksien puitteissa. Järjestelmissä on käyttöoikeus tasoja eri työroolien toteuttamiseksi. Eräs pääkäyttäjistä totesi, että hänen vastaamansa järjestelmän käyttöoikeudet on annettu työtehtävien mukaan. Ongelmana on se, että työtehtäviä joudutaan arviomaan osin tehtävänimikkeen perusteella eikä samalla nimikkeellä työskentelevillä henkilöillä aina ole kaikissa työpisteissä sama työnkuva. Joissakin tapauksissa nimikkeestä ja siihen liittyvästä yleisestä tehtävänkuvauksesta riippumatta työntekijän tehtävät on saatettu räätälöidä tapauskohtaisesti. Tästä saattaa mahdollisesti seurata samalla nimikkeellä olevien työntekijöiden osalta joko tarpeettoman laajoja tai rajattuja käyttöoikeuksia heidän todellisiin työtehtäviinsä nähden.

Pääkäyttäjille kysyttiin, onko vaaralliset työyhdistelmät tunnistettu heidän vastuullaan olevassa järjestelmässä. Pääkäyttäjien haastattelun perusteella vaarallinen työyhdistelmä-käsite oli epäselvä eikä vaarallisia työyhdistelmiin ole ilmeisesti kiinnitetty riittävästi huomiota.

Kysyttiin myös onko olemassa sellaisia työyhdistelmiä (käyttöoikeuksia), jossa tarvitaan kahden tai useamman henkilön hyväksyntä. Haastateltujen pääkäyttäjien ylläpitämissä järjestelmissä esimies aina anoo ja hyväksyy käyttöoikeudet alaisilleen. Yksi pääkäyttäjistä totesi, että hänen vastaamansa järjestelmän käytön yhteydessä käyttäjät tarvitsevat myös toisen järjestelmän käyttäjätunnuksia ja käyttöoikeuksia. Tämän järjestelmän käyttäjätunnus- ja käyttöoikeudet antaa toinen taho eli esimies hakee alaisilleen erikseen käyttäjäntunnukset ja käyttöoikeudet tämän järjestelmän pääkäyttäjältä.

6.3 Tutkimuskysymyksien merkittävyys

Tässä kappaleessa pyritään tuomaan lyhyesti esille yhteenvetona tutkimuksen perusteella hahmottaman analyysin käyttäjäidentiteettien ja käyttäjävaltuuksien hallintajärjestelmän hyödyistä, riskeistä sekä hyväksi katsoman tavoitetilan.

Hyvänä asiana näkisin, että käyttäjähallintaan ja käyttövaltuuksiin liittyvä haaste on tunnistettu sekä sisäisen tarkastuksen että tietohallinnon toimesta. Tietohallinnolla on tavoitetila sekä vaatimuksia käyttäjähallintajärjestelmälle, joka tehtiin IAM- järjestelmätarjouspyynnön yhteydessä.

Tietohallinto on seurannut aktiivisesti markkinoilla olevia käyttäjähallintajärjestelmien tarjontaa. Vuodenvaihteessa 2011–12 oli vireillä koko kaupungin tietojärjestelmät kattavan käyttäjähallinta- ja kertakirjautumisratkaisun kilpailutus. Tuolloin ei kuitenkaan olosuhteiden muutoksesta johtuen päädytty järjestelmähankintaan, vaan päätettiin edettävän käyttäjähallinnan kehittämisessä vähitellen pitkällä aikajänteellä. Syksyllä 2012 Kuntaliitto käynnisti osana kuntien kokonaisarkkitehtuurityötä käyttövaltuushallinnan viitearkkitehtuurin määrittelytyön, johon Vantaan kaupunki osallistuu.

Pääkäyttäjillä on hyvä käyttöoikeuksien käsitteiden tuntemus ja laaja asiantuntemus. Sekä tutkimuskysely että haastattelut osoittivat kuitenkin, että esimiesten keskuudessa on osaamispuutteita käyttöoikeuksien käsitteiden ja sisällön tuntemisessa sekä alaisten työkuvien muutosten vaikutuksista käyttöön. Ongelmana voidaan pitää sitä, että kaikkien järjestelmien osalta käyttöoikeushallintajärjestelmää ei ole keskitetty. Toisaalta tämä ei välttämättä ole käytännössä kaikilta osin mahdollista eikä mielekästä teknisistä- tai kustannussyistä joissakin järjestelmissä työtehtäviin nähden sopimattomasti määriteltyjen käyttöoikeuksien havaitsemiseen ja vaarallisten työyhdistelmien torjumiseen liittyviä keinoja ja työkaluja olisi kehitet-

tävä. Käyttäjähallinta- ja käyttöoikeusprosesseja kehitettäessä IAM- kokonaisprosessi pitää ottaa huomioon liiketoimintaprosessien sekä käyttäjähallintastrategian lähtökohdasta. Tällöin nämä haasteet saattavat korjautua.

Tarpeettoman laajat tietojärjestelmien käyttöoikeudet ovat tietoturvariski. Kaupungin tasolla johdon riittämätön sitoutuminen käyttäjähallinnan strategian läpiviemiseen on merkittävä haaste. Nyt ongelmien ja riskien tunnistaminen on osa organisaation käyttäjätunnus- ja käyttöoikeushakuprosessin kehittämistä uudella tavalla. Kehitystyön läpivienti ei pidä olla yksin tietohallintolähtöinen vaan liiketoimintaprosessien omistajien vetämä sekä johdon tukema. Liiketoimintaprosessinomistajilla on osaamista heidän palveluunsa liittyvistä tietoturva- ja lainsäädäntövaatimuksista. Tietohallinnon pitää tehdä enemmän yhteistyötä ja tutkia markkinoilla saatavilla olevien käyttäjähallintajärjestelmien eri ratkaisuja.

7 Johtopäätökset

Tämän tutkimuksen tavoite on vastata kysymykseen, miten esimiehet ymmärtävät käyttöoikeushakuprosessin ja sen sisällön. Selvitys tehtiin sisäisen tarkastusraportin ja oman osaamisen pohjalta laadituilla kysymyksillä sekä kolmea pääkäyttäjää haastattelemalla. Tutkimuskysely toteutettiin Webropol-nimisellä ohjelmalla, jolla tehtyyn kyselyyn pystyi vastaamaan Internet-selaimella. Tutkimuskyselyn vastaamispyyntö lähetettiin esimiehille sähköpostitse.

Yleisesti ottaen esimiehet tunnistavat käyttöoikeushakuprosessin pääpiirteet. Vastaajista 80 % oli sitä mieltä, että he tietävät millainen käyttäjätunnus- ja käyttöoikeushakuprosesseja organisaatiossa on käytössä. Tästä huolimatta yli puolet vastasi tietohallinnon palvelukeskuksen myöntävän käyttäjätunnukset ja käyttöoikeudet, mikä ei pidä paikkansa. Esimiesten keskuudessa on osin väärä käsitys tietohallinnon ja pääkäyttäjien rooleista ja vastuista. Tietohallinnon vastuu on vastata tieto- ja viestintäteknologia (Information and communications technology ICT) palvelutuotannosta yhteistyössä toimialojen sidosryhmien kanssa. Tietohallinto ei vastaa työntekijöille haettavien käyttöoikeuksien hyväksynnästä, vaan osaltaan käyttöoikeushallintaprosessin toteutuksesta ja käyttäjähallintajärjestelmän kehittämisestä. Pääkäyttäjä puolestaan vastaa tietyn järjestelmän pääkäyttäjätehtävistä, eikä hänellä ole hyväksymisoikeutta esimiehen alaisen käyttöoikeuksiin. Esimiehellä on vastuu arvioida, mitkä käyttöoikeudet hänen alaisillaan pitää olla kussakin järjestelmässä.

Erään haastattelemani pääkäyttäjän mukaan esimiehet olettavat, että koska tietohallinto luo esimerkiksi verkkotunnuksia, tietohallinto käsittelee ja hyväksyy myös kaikkien tietojärjestelmien käyttöoikeudet. Näin ei ole todellisuudessa. Tietohallinnolla ei ole pääsääntöisesti mitään oikeuksia toimialojen käytössä oleviin tietojärjestelmiin, niiden käyttäjähallinta -tai käyttöoikeusjärjestelmiin.

Organisaatiossa käyttöoikeuksien myöntämisestä päättää ensisijaisesti oma esimies. Tietyissä tapauksissa pääkäyttäjä tarkistaa esimiehen hyväksymät käyttöoikeuspyynnöt, jottei esimies hyväksy liian laajoja käyttöoikeuksia. Käyttöoikeuksien sisällön selvittämiseksi esimiehet ovat yleensä yhteydessä pääkäyttäjään, tukipalveluun tai ovat kysyneet apua kollegalta. Lisäksi suurin osa vastaajista oli sitä mieltä, että käyttäjätunnus- ja käyttöoikeushakuprosessi aiheuttaa ylimääräistä työtä. Tämän perusteella esimiehet muiden työtehtäviensä aiheuttaman kiireen ja kuormituksen vuoksi eivät todennäköisesti paneudu riittävästi alaisilleen pyytämien käyttöoikeuksien sisältöön, laajuuteen ja muutostarpeisiin työtehtävien muutoksien mukaisesti. Tämä saattaa aiheuttaa tietoturvariskejä, jos alaisille haetaan laajemmat käyttöoikeudet, kuin on työtehtävien hoitamiseksi tarpeen tai hänelle jää esimerkiksi vanhan työtehtävän perua liian laajat käyttöoikeudet. Lisäksi saattaa olla, että työtehtäviä määriteltäessä ei ole otettu huomioon vaarallisten työyhdistelmien muodostumisen syntymistä, mikä aiheuttaa

osaltaan liian laajojen käyttöoikeuksien hakemista alaisille. Seuraavassa taulukossa 8 pyritään tuomaan yhteenveto johtopäätöksestä. Yhteenvetotaulukon on tarkoitus kirkastaa miten tutkimuskysymykset ovat analysoitu ja toimenpide-ehdotukset on esitetty yhteenvetona.

Tutkimuskysymys	Analyysiin tulos	Yhteenveto
Miten käyttäjätunnuksien- ja käyttöoikeuksien haku- ja käsittelyprosessi tunnetaan?	80% kokee tuntevansa käyttöoikeushakuprosessin. Yli 50% vastasi tietohallinnon palvelukeskuksen myöntävän käyttäjätunnukset ja käyttöoikeudet, mikä ei pidä paikkansa.	Esimiehet tuntevat käyttöoikeushakuprosessin pääpiirteet. Esimiesten keskuudessa on osin väärä käsitys tietohallinnon ja pääkäyttäjien rooleista ja vastuista.
Mikä koetaan epäselväksi käyttäjätunnuksien- ja käyttöoikeuksienhaku- ja käsittelyprosessissa?	Käyttöoikeushakuprosessi ei ole kuvattu, alaisille haettavien käyttöoikeuksien sisältö ja laajuus eivät ole selkeitä. Käyttöoikeudet haetaan eri tavoin, eli ei ole yhteneväisiä. Käyttöoikeudet eri paikasta, eikä ole yhtä paikkaa, josta haetaan kaikkia käyttöoikeuksia (ns. verkkokauppa tai itsepalveluportaali). Henkilön työn alkaessa ei ole vielä selvillä, mitä kaikkea hänen tehtäviin kuuluu.	Käyttöoikeuksien sisällön selvittämiseksi esimiehet ovat yhteydessä pääkäyttäjään tai tukipalveluun tai ovat kysyneet apua kollegalta. Prosessi aiheuttaa ylimääräistä työtä. Esimiehet eivät paneudu riittävästi alaisilleen pyytämien käyttöoikeuksien sisältöön, laajuuteen ja muutostarpeisiin työtehtävien muutoksien mukaisesti.
Onko jossain organisaation osassa erityisiä haasteita käyttäjätunnus- ja käyttöoikeushallintaprosessin suhteen?	Tutkimuskysymyksiin vastanneista suurin osa on sosiaali- ja terveystoimesta sekä sivistystoimesta. Toimialoilla on käytössä erilaisia järjestelmiä. Organisaation henkilöstön vaihtuvuus on suuri.	Saattaa aiheuttaa tietoturvariskejä. Alaisille haetaan laajemmat käyttöoikeudet, kun on työtehtävien hoitamiseksi tarpeen. Alaisille jää esimerkiksi vanhan työtehtävän peruna liian laajat käyttöoikeudet.
Miten mahdollinen tiedonpuute ja mahdolliset virheelliset käsitykset käyttäjätunnuksien ja käyttöoikeuksien hakuprosessista vaikuttavat organisaation toimintaan ja tietojärjestelmien käyttöön?	Vaarallisten työyhdistelmien muodostumisen syntymisenä. Osaltaan liian laajojen käyttöoikeuksien hakeminen alaiselle mahdollistuu.	Vaarallisten työyhdistelmien määritys pitää tehdä sekä esimiehien pitää ymmärtää sen käsite. Säännöllinen ajan tasalla oleva raportti esimiehelle alaisten käyttöoikeuksista on tarpeellinen.
Tutkimuksen merkitys on, että saatuja tuloksia hyödyntämällä voidaan parantaa käyttäjätunnus- ja käyttöoikeushakuprosessia sekä kiinnittää huomiota esimiesten ymmärryksen syven-	Tutkimusvastauksista saatiin myös kehittämisehdotuksia ja palautetta nykyisestä organisaation käyttöoikeuksien sisällön ymmärtämisestä. Myöskin käyttöoikeushaku- ja hyväksyntäprosessin toimivuudesta.	Esimiehet tarvitsevat selkeät ja ajan tasalla olevat ohjeet sekä opastusta. Organisaation pitää kehittää käyttöoikeushallintaprosesseja, käyttöoikeuksien sisältöä ja kiinnittää

tämiseen käyttöoikeuksien sisällöstä ja laajuudesta.		huomiota vaarallisiin työyhdistelmiin. Käyttäjien tarpeen täyttämisen kannalta on merkittävää ottaa huomioon saadut kehityskommentit ja sen perusteella tuoda uusi lähestymistapa käyttöoikeushakuprosessiin ja käyttöoikeuksien sisältöön.

Taulukko 8: Yhteenveto johtopäätöksestä

7.1 Tutkimuksen tuotos käyttöoikeushallinnalle

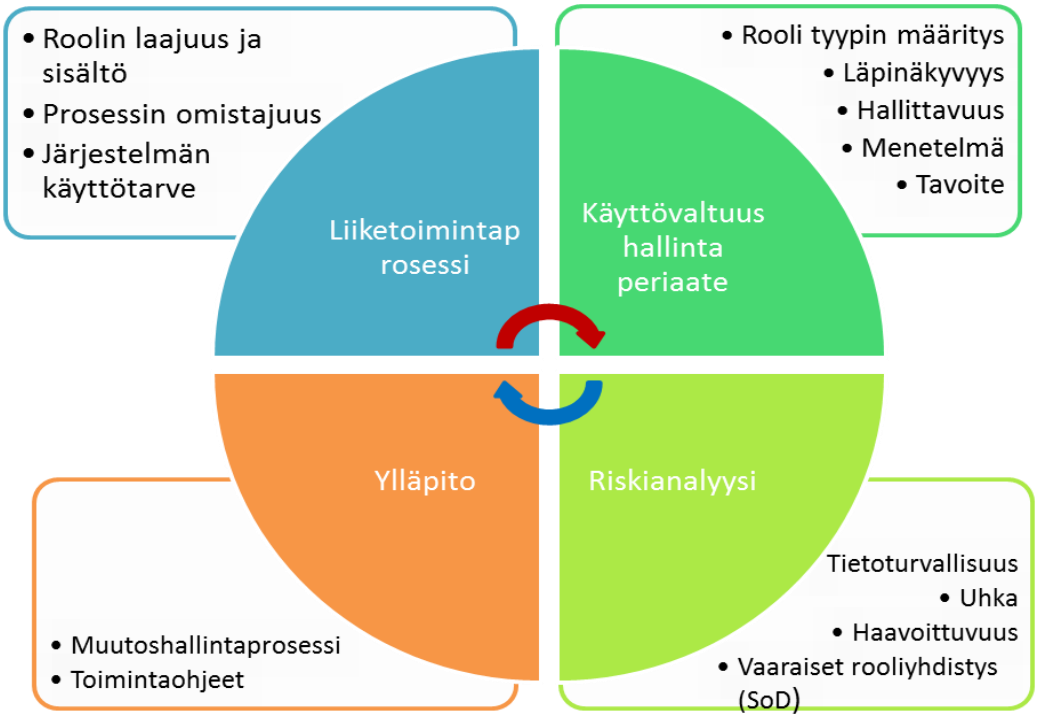
Tämän tutkimuksen lopputulosta on tarkoitus hyödyntää organisaation identiteetin- ja pääsyhallintaa kehitettäessä. Tutkimus osoitti, että käyttöoikeuksien merkityksestä esimiehillä ei ole välttämättä riittävästi tietoa. Esimiehet eivät joko pysty tietämään tai ehdi paneutumaan siihen, mitkä ovat heidän alaiselle esittämien käyttöoikeuksien laajuudet, niiden mahdollistamat toiminnot, kuinka sopiva käyttöoikeus on alaisella suhteessa hänen työtehtäviinsä sekä kuka on kyseisen järjestelmän käyttöoikeuksien yhdyshenkilö. Tämä on tietoturvariski ja lisäksi käyttöoikeuksien haku ja käsittely on hidasta. Alaisten työkuvan muuttuessa esimiehet eivät pysty tietämään, mitkä käyttöoikeudet heidän alaisillaan on ollut edellisessä työtehtävässään, mikäli alainen on siirtynyt työyksiköstä toiseen. Pääkäyttäjien näkemyksen mukaan esimiehet tarvitsisivat nykyistä selkeämpää, ajan tasalla olevaa ohjeistusta käyttöoikeuksien sisällöstä sekä tietämystä, siitä mikä käyttöoikeus soveltuu mihinkin tehtävään.

Näiden haasteiden ratkaisemiseksi olen suunnitellut organisaatiossa käyttöoikeuksien kuvaamista varten mallia ”käyttöoikeusprofiili”, jolla helposti pystyy kuvamaan esimiehen käyttöoikeuksia alaiselleen hakiessaan tarvitsemia käyttöoikeuksien tietoja. Tämä käyttöoikeusprofiili on standardoitu malli, jolla pystyy esittämään järjestelmän roolit. Standardimallipohja mahdollistaa sen, että esimies saa samanlaisen näkymän kaikista rooleista ja pystyy ymmärtämään minkä tahansa roolin sisällön ja laajuuden. Käyttäjätunnuksia ja käyttöoikeuksia haetttessa itsepalveluportaalin kautta, niihin liittyvät kaikki roolit olisi kuvattava käyttöoikeusprofiilimallin mukaisesti.

Käyttöoikeusprofiilin viitekehyksen periaate on selkeyttää loppukäyttäjille tai esimiehille käyttöoikeuksien sisältöä ja niiden laajuutta. Se antaa raamin käyttöoikeusylläpidon hallinnalle niin, että roolimuutos tehdään aina muutoshallinnan kautta. Lisäksi käyttöoikeusprofiilin ansiosta pystyy tunnistamaan vaaralliset rooliyhdistelmät ennalta määriteltynä sekä arvioimaan ja hallitsemaan riskejä. Käyttöoikeusprofiilin standardoinnilla minimoidaan käyttöoikeuksien ylläpitoa sekä niiden kehittäminen tulee helpottumaan. Lisäksi poistuu esimiesten tur-

hat yhteydenotot tukipalveluun sekä ylimääräistä aikaa vievä selvittely siitä, mitkä käyttöoikeudet pitää hakea alaisille, vähentyy. Myös käyttöoikeuksiin liittyvä käyttötuen määrä minimoituu ja samalla kustannukset pienenevät.

Käyttöoikeusprofiilin viitekehyksen suunnitelmassani otin neljä erilaista näkökulmaa, jotka tukevat tietoturvallisuuden parantamista sekä kasvattavat käyttöoikeuksien haun ja käsittelyn tehokuutta. Näkökulmat on kuvattu kuvion 23 avulla.



Kuvio 23: Käyttöoikeusprofiilin kuvaamista varten tarvittavat näkökulmat

A. Liiketoimintaprosessi

Davenport & Shortin (1990) mukaan liiketoimintaprosessi on joukko toisiinsa liittyviä tehtäviä ja niiden toteuttamiseen tarvittavia resursseja, joiden avulla saadaan aikaa liiketoimintatulokset. Pall (1987) puolestaan määrittelee, että liiketoimintaprosessi on menetelmä "loogisen organisaation ihmisiä, materiaaleja, energiaa, laitteita ja menettelyjä, jotka ovat suunniteltu osaan työtehtäviä jolla voi tuottaa tietyn lopputuloksen (työ tuote)". (Davenport & Short 1990, 11-27; Pall 1987, 434-435.)

Organisaation liiketoimintaprosessin omistaja suunnittelee ja määrittää sovelluksien vaatimuksia. Yleensä kyseinen yksikkö suunnittele, minkälaisia käyttöoikeuksia tarvitaan tietyssä sovelluksessa liiketoimintaprosessisin tavoitteen toteuttamiseksi. Omistajayksikkö määrittele

käyttöoikeuden kuvauksen, laajuuden, mahdolliset toiminnot tai tapahtumat, hyväksyntäprosessin ja kyseisen käyttöoikeuksien yhdyshenkilön. Liiketoimintaprosessin omistajalla on enemmän tietoa siitä, mitkä käyttöoikeudet mahdollistavat minkälaisia toimintoja erilaisissa sovelluksissa. Käyttäjätunnus ja käyttöoikeushakuprosessin kehittäessä järjestelmän prosessiomistajan toimesta tehdään käyttöoikeusmääriteltyyn ja tietohallinto tukee teknisestä toteutuksesta.

Toisena liiketoiminta näkökulmana on henkilöstöhallinnon rooli. Tietohallinto, henkilöstöhallinto ja järjestelmän omistava taho yhteistyössä kuvaavat henkilön työkuvan ja mitkä järjestelmät hänen työkuvaan kuuluvat. Tällä pystytään varmistamaan, että esimiehellä on selvä ymmärrys käyttöoikeuksien määrittelyn merkityksestä uutta henkilöä palkattaessa. Henkilöstöhallinnon rooli on erittäin merkittävä, jotta esimiehet suoriutuvat sovittun käytännön mukaisesti. Seuraavassa taulukossa 9 on otettu esille käyttöoikeusprofiili standardimallin ylätasot. Tämä standardimalli on laajasti kuvattu liitteessä 9.

Roolin profiili	
Yhteistiedot	Nimi, järjestelmä, tekninen nimi, moduuli, kuka voi anoa, kuka hyväksyä, hyväksyntätaso, roolityyppi/ roolin tyyppi ja virka-asema
Toiminnallinen kuvaus	Tehtävien hoitamisen liittyvät oikeudet ja raportit
Roolin laajuus / rajaus	Organisaatiotaso/ yritystaso/ PK/ kustannuspaikka
Mitä toimintoja roolissa on?	Luo, muokkaa, poistaa jne...
Vaarallinen rooliyhdistelmä	Rooli01, rooli02,rooli03
Roolista lisätietoa antaa	Omistajaorganisaatio, yhteyshenkilö, puh, sähköposti

Taulukko 9: Käyttöoikeusprofiilin standardimallin luomiseksi ylätasokuva

B. Käyttövaltuushallintaperiaate

On perustettava käyttäjähallintakonsepti koko organisaation tasolle. Käyttäjähallintakonseptin tarkoitus on kuvata organisaation käyttäjä- ja käyttöoikeushallinta eri järjestelmien tasolla. Käyttäjähallintakonseptin pää osa- alueet ovat kuvattu seuraavassa taulukossa 10.

Osa-alueet	Selitys
Käyttövaltuutushallintajärjestelmän kuvaus	Kuvataan käyttäjille miten käyttöoikeuksia haetaan ja hyväksytään.
Käyttövaltuuspolitiikka	Määritellään kuka mitäkin voi tehdä ja millä valtuudella.
Käyttäjätunnuksien elinkaarihallinnan kuvaus	Kuvataan miten ja millä periaatteella tunnus syntyy, passivoidaan ja poistetaan.
Salasana politiikka	Määritellään kuinka usein pitää vaihtaa salasana ja niiden monimutkaisuus.
Järjestelmien luokitus ja integraation kuvaus	Jokaisen käyttäjähallintapiirissä olevien järjestelmien luokitus sekä integraatio toteutuksen kuvaus.
Roolien toteutus- ja rajausperiaatteet	Kuvataan miten käyttöoikeus luodaan, päivitetään ja poistetaan järjestelmästä sekä kaikki organisaatiossa käytössä olevat käyttöoikeuksien rajausperiaatteet kuvataan erikseen.
Kriittisten oikeuksien hallinta	Tiettyjen kriittisten käyttöoikeuksien hallinta kuvataan erikseen, miten niitä haetaan ja hyväksytään.
Vaarallisten työyhdistelmien hallinta ja valvonta	Organisaatiossa olevien erityisesti kriittisten järjestelmien osalta kuvataan millainen käyttöoikeuksien yhdistelmä on vaarallinen työyhdistelmä.
Roolien kehitys-, muutoshallinta sekä muutoksesta tiedottaminen	Käyttöoikeuksien roolit, muutoshallintaprosessit ja niiden toteuttaminen kuvataan (kuka tekee mitäkin).

Taulukko 10: Käyttäjähallintakonseptin pääosa-alueet

Käyttäjähallintakonseptin eräs keskeinen osa-alue on käyttöoikeushallintajärjestelmä, jossa määritellään käyttövaltuushallintaperiaatteet, käyttöoikeushaku- ja myöntämisprosessi yhteistyössä järjestelmän pääkäyttäjän kanssa. Jokaisen järjestelmän käyttöoikeuksien profiili pitää määritellä selkeästi siten, että on selvää, mitä käyttöoikeudet sisältävät, niiden laajuus ja voimassaoloaika käyttövaltuushallintajärjestelmän hakulomakkeessa. Lisäksi käyttöoikeuksien myöntämisprosessi pitää kuvata selkeästi, siten että on määritelty kuka myöntää yksittäisen tietojärjestelmän käyttöoikeudet ja kuinka kauan hyväksyntäkäsittely kestää.

C. Ylläpito ja muutoshallinta

Tietohallinnon pitää tukea prosessiomistajien käyttövaltuushallintaprosessitoimintaa sekä käyttöoikeuksien ylläpitotehtäviä. Käyttäjäroolien kehitys- ja muutos pitää toteuttaa suunnitellusti ja hallitusti. Roolien muutoksien yhteydessä pitää noudattaa sovittua muutoshallintaprosessia ja varmistaa, ettei muutos tuota minkäänlaisia vaarallisia rooli- tai käyttöoikeusyhdistelmiä. Usein roolimuutos tehdään liiketoimintaprosessin omistajien kanssa, jotta pystytään varmistamaan, että kaikille osapuolilla on tietoa muutoksen sisällöstä.

D. Tietoturva näkökulma (Riskinanalyysi)

Organisaatiossa on tärkeää toteuttaa tietoturvapolitiikkaa, joka tukee liiketoimintaprosessia ja järjestelmien käyttökulttuuria. Organisaation käyttäjähallintakonsepti noudattaa tietoturvapolitiikkaa sekä tunnistaa mahdollisia organisaation tietoturvariskejä mm. vaaralliset rooli- tai käyttöoikeusyhdistelmät. Käyttöoikeuskonseptin tietoturvallisuutta pitää arvioida säännöllisesti ja todeta kriittisimmät kehityskohteet. Käyttöoikeuskonsepti antaa reunaehdotuksia pääkäyttäjille ja järjestelmän ylläpitäjille sen, että käyttäjillä ei ole liikoja käyttöoikeuksia. Tilapäistyöntekijöiden käyttöoikeuksien voimassaoloaika määritellään etukäteen. Käyttöoikeusprofiilin avulla esimies pystyy tietämään vaaralliset rooliyhdistelmät ennen kuin hakee tai hyväksyy niitä alaisilleen. Lisäksi, kun järjestelmän käyttöoikeusprofiili on määritelty ja viety IDM- itsepalvelujärjestelmään, niin järjestelmän avulla vaarallisten rooliyhdistelmät pystytään torjumaan ennalta. Liitteessä 9 on eräs esimerkki laajasti kuvatusta järjestelmäroolista.

7.2 Tulosten luotettavuus

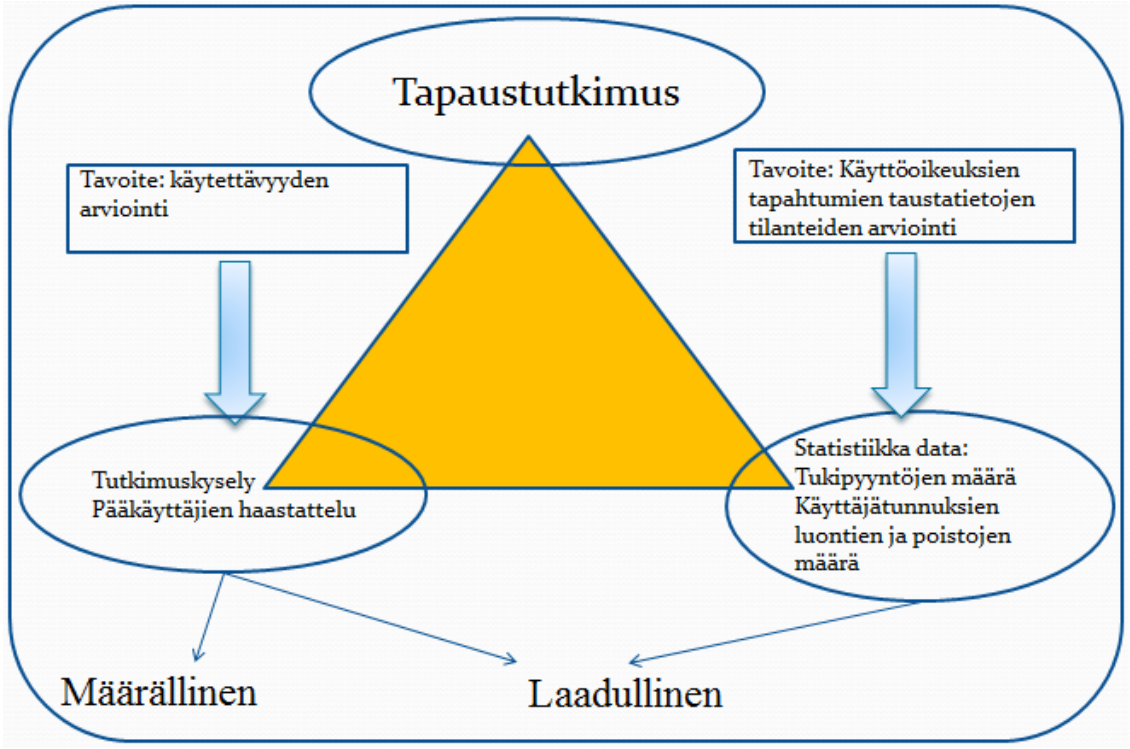
Yin (2009) korostaa tutkimuksen menetelmänä käytettyjen useiden lähteiden tärkeyttä. Ne muodostavat aineistotriangulaation, jossa empiirisestä aineistosta esiin nousevat tulokset tukevat toisiaan ja lisäävät tutkimuksen luotettavuutta verrattuna tutkimukseen, jossa tulokset pohjautuvat vain yhteen aineistoon. Miles & Huberman (1994) puolesta tutkimuksen objektiivisuuden kannalta eräs olennaisista kysymyksistä on: onko tutkimuksen yleiset menetelmät ja menettelyt kuvattu selkeästi ja yksityiskohtaisesti ts. tuntuuko siltä, että tutkijalla on kokonaiskuva mukaan lukien ”kulissien takaista” tietoa. Tärkein peruste tutkimukselle on se, että tutkijalla on aikaa ja taitoja kehittää totuuden arviota, jolla on vankempi todiste kuin maalaisjärjellä. Johtopäätöksen peruskysymyksen parasta osaa voidaan lähestyä "justificatory" oikeuttamisperusteen näkökulmasta eli ne arvot ja tavoitteet, joita sillä pyritään toteuttamaan. (Yin 2009, 116; Miles and Huberman 1994, 276.)

Kokonaisen tapaustutkimuksen pitäisi osoittaa vakuuttavasti se, että tutkija pyrkii laajentamaan kattavasti olennaisten todisteiden keräämisestä. Kokonaistavoite on silti vakuuttaa luki-

ja, että olennaiset todisteet pysyivät koskemattomana tutkijan toimesta ottaen huomioon tapaustutkimuksen rajat. (Yin 2009, 186–187.)

Guba & Lincoln (1994) esittävät, että kvalitatiivisen tutkimuksen luotettavuus riippuu tutkimustuloksien merkittävyydestä eli ovatko tutkimustulokset otettu esille hyvin tai ne ovat huomioonottamisen arvoisia. Tutkijan on kyettävä vakuuttamaan lukijansa ottamalla tutkimuksen tuottavat löydökset, implikaatiot esille paremmin. Tässä tutkimuksessani on tuotu esille aineistokeruun analysoinnissa olennainen tutkimuskohde, eli käyttöoikeushakuprosessin ymmärrystä esimiesten keskuudessa. (Guba & Lincoln 1994, 117–295.)

Tutkimuksessani on keskitytty käyttäjäidentiteettien ja käyttövaltuushallintaprosessin periaatteisiin ja hyvät käytännöt käsitellään eri näkökulmista: esimiehen, loppukäyttäjien, pääkäyttäjien, ylläpitäjien, tietohallinnon, mutta myös tietoturvan ja oikeusturvan näkökulmasta. Tutkimusaineiston keräämisen menetelmänä käytettiin kyselyä, haastattelua ja taustaaineistoja. Mielestäni nämä menetelmät muodostavat toisiaan tukevan kokonaisuuden Yin:in kuvaaman aineistoriangulaation ja lisäävät tutkimustuloksen luotettavuutta. Scholtz, Cilliers & Calitz (2010) viittaavat, että Jutrasin (2004) aineistontriangulaatio lähestymistapa (tässä tapaustutkimuksessa: tutkimuskysely, pääkäyttäjähaastattelut ja tukipyyntöjen ja käyttäjätunnuksien luontien ja poistojen tausta –aineisto) saattaa olla helpoin ymmärtää mikä tekee uudesta sosioteknisestä järjestelmästä onnistuneen (kuvio 24). Scholtz, Cilliers & Calitz (2010) vahvistavat, että kaikille tutkimusmenetelmillä on vahvuuksia ja heikkouksia. Yhdistämällä kaksi tai kolme eri menetelmää tutkija voi saada paremman käsitykseen ilmiöistä, jotka voivat jäädä huomaamatta kun käytetään vain yhtä tutkimusmenetelmä. Scholtz, Cilliers & Calitz 2010, 287; Jutras 2004.)



Kuvio 24: Aineistontriangulaatio lähestymistapa laadullisen tutkimuksen keinoin mukailen (Scholtz, Cilliers & Calitz 2010, 287)

Syrjälän, Ahosen, Syrjäläisen & Saarien (1996) mukaan käsitteiden epäselvyys saattaa vääristää tuloksia jo aineistonkeruun aikana. Haastateltavan ja haastattelijan tulisi puhua samoista asioista samoilla käsitteillä. Käsitteiden epäselvyys vaikeuttaa aineiston analysointia, joka heikentää tutkimuksen luotettavuutta. Jos lukijalle jäävät epäselviksi tutkimuksen keskeiset käsitteet, raportin tulos epäonnistui. (Syrjälä, Ahonen, Syrjäläinen & Saari 1996, 100.)

Kyselyyn vastanneiden valinta perustui heidän esimiesasemaansa. Lähes kaikki organisaation esimiehet tekevät työsopimuksia ja hakevat tai hyväksyvät alaisilleen käyttäjätunnuksia ja käyttöoikeuksia eri tietojärjestelmiin. Siksi tutkimuskyselyn lähettäminen esimiehelle oli luonteva valinta. Kuitenkin kaikista esimiehistä valittiin ne esimiehet, jotka tekevät käyttäjätunnus- ja käyttöoikeuspyyntöjä omille alaisilleen organisaation käyttöoikeushakua varten käytössä olevasta järjestelmästä. Kyselyyn vastanneista 64 esimiehestä 70 % on ollut yli kuusi vuotta Vantaan kaupungin palveluksessa. Näillä 70 %:lla on kuudesta yli viiteentoista vuotta esimieskokemusta (kuvio 10).

Eli näillä esimiehillä on hyvä tuntemus organisaatiosta ja vankkaa esimieskokemusta. Monen vuoden organisaatiossa esimiesasemassa työskenteleminen on antanut heille kokemusta ja käsityksen organisaatiossa sovellettavasta tietojärjestelmien käyttöoikeusprosessista. Näiden

kokemuksien ansioista kyselyyn vastanneilla esimiehillä on vahvaa tietoa kyselyn aiheesta ja sen myötä tuloksen voidaan olettaa olevan luotettava.

7.3 Kehitysehdotukset

On varmistettava, että käytössä olevien järjestelmien käyttöoikeudet ovat ajan tasalla ja kuvattu selkeästi esimiehille. Esimiesten on myös syytä itse tutustua käyttöoikeushakuprosessiin liittyviin ohjeisiin ja paneutua alaistensa tarvitsemien käyttöoikeuksien sisältöön. Vastuu alaisille haettavista käyttöoikeuksista on aina esimiehellä. Esimiehen oman oikeusturvan kannalta esimiehen on syytä olla tietoinen siitä, mitä käyttöoikeuksia alaisilla saa olla suhteessa työtehtäviin.

Haastattelemani pääkäyttäjien näkemys ja tutkimuskysymyksien tulokset ovat melko samansuuntaisia. Suuri haaste on, että organisaatiossa ei ole automatisoitua käyttöoikeushallinta- ja käyttövaltuushallintajärjestelmää. Siitä syystä käyttöoikeuksia haetaan erilaisia kanavia käyttäen. Tästä syystä organisaatiossa ei noudateta yhdenmukaista käyttöoikeushaku- ja hyväksyntäprosessia, eikä ole keskitettyä organisaation sisäistä verkkopalvelua, jossa käsiteltäisiin käyttöoikeuksiin liittyviä pyyntöjä ja hyväksyntöjä.

Tutkimuskysymyksiin vastanneista suurin osa on sosiaali- ja terveystoimesta sekä sivistystoimesta. Näillä toimialoilla on käytössä erilaisia järjestelmiä, ja lisäksi organisaation henkilöstön vaihtuvuus on suuri, mistä seuraa haasteita käyttäjätunnusten ja käyttöoikeuksien hallinnassa. Tutkimustuloksen luotettavuuden kannalta on hyvä, että suurin osa vastaajista oli sosiaali- ja terveystoimesta ja sivistystoimesta, koska kaupungin kokonaishenkilöstömäärästä noin 68 % työskentelee sivistystoimessa ja sosiaali- ja terveystoimessa.

Tutkimusvastauksista saatiin myös kehittämisehdotuksia ja palautetta nykyisestä organisaation käyttöoikeuksien sisällön ymmärtämisestä, käyttöoikeushaku- ja hyväksyntäprosessin toimivuudesta. Kaiken kaikkiaan tämän tutkimuksen aikana tutkimuksen tekijä ymmärsi, että esimiehet tarvitsevat selkeät ja ajan tasalla olevat ohjeet sekä opastusta. Organisaation pitää kehittää käyttöoikeushallintaprosesseja, käyttöoikeuksien sisältö ja kiinnittää huomiota vaarallisiin työyhdistelmiin. Käyttäjien tarpeen täyttämisen kannalta on merkittävää ottaa huomioon saadut kehityskommentit ja sen perusteella tuoda uusi lähestymistapa käyttöoikeushakuprosessiin ja käyttöoikeuksien sisältöön.

Tästä syystä on aiheellista selvittää, miten voisi kehittää käyttöoikeushakuprosessia ja millä keinoilla voisi esittää käyttöoikeuksien sisältö esimiehille ymmärrettävällä tavalla. Lisäksi on hyvä kertoa esimiehille, kuinka merkittävässä asemassa he ovat tietojärjestelmien käyttöön liittyvien tietoturvariskien vähentämisessä tältä osin. Erityisesti tietoturvan parantamiseksi

IT-roolien ja työroolien yhdistelmien määrittely sekä vaarallisten työyhdistelmien tunnistaminen ja niiden riskien arviointikuvauksen tekeminen on aiheellista.

Tutkimuksen lähestymistapa tuo Vantaan kaupungille uuden näkökulma käyttäjätunnus- ja käyttöoikeushakuprosessin kehittämiseen. Tutkimus antaa osaltaan ideoita käyttäjätunnus- ja käyttöoikeushakuprosessin kehittämiseen. Tutkimuksen tuloksia hyödyntämällä voidaan parantaa käyttäjätunnus- ja käyttöoikeushakuprosessia sekä kiinnittää huomiota esimiesten ymmärryksen syventämiseen käyttöoikeuksien sisällöstä ja laajuudesta. Lisäksi sitä myöden organisaation tietoturva parantuu huomattavasti sekä nykyinen kuukausittaisen tilaston mukaan n. 39 % käyttäjähallintaan liittyvät tukipyynnöt vähentyvät merkittävästi.

Jatkotutkimusaiheena voisi olla, miten käyttäjätunnus- ja käyttöoikeushakuprosessien laatua parannetaan hyödyntämällä itsepalveluportaalia sekä miten prosessin laadun parantaminen näkyy esimiesten keskuudessa. Tutkimuksen kohteeksi voisi asettaa käyttäjätunnus- ja käyttöoikeusprosessin. Toinen aihe jatkotutkimukselle voisi olla vaaralliset työyhdistelmät, miten voidaan identiteetti- ja pääsyhallintajärjestelmällä parantaa organisaation tietoturvaa. Tutkimuskohteeksi voisi ottaa myös vaarallisten työyhdistelmien valvonnan.

Lähteet

Painetut teokset

Ackoff, R. L., Gupta, S. K., & Minas, J. S. 1962. Scientific Method. New York: John Wiley & Sons, Inc.

Arden, B. W. (ed.) 1980. "What can be automated?" The Computer Science and Engineering Research Study (COSERS). Cambridge, MA: MIT Press.

Avison, D. E., Lau, F., Myers, M., & Axel Nielsen, P. 1999. Action research to make academic research relevant, researcher should try out their theories with practitioners in real situations and real organizations. Communications of the ACM, 42(1), 94–97.

Bailey, K. D. 1982. Methods of Social Research. New York: The Free Press.

Basili, V. R., Selby, R. W., & Hutchens, D. H. 1986. Experimentation in software engineering. IEEE Transactions on Software Engineering SE-12, 7, 733-743.

Benbasat, I. An analysis of research methodologies. 1984. The Information Systems Research Challenge, W. F. McFarlan, ed. Cambridge, MA: Harvard Business School Press, 47-85.

Blake, S. P. 1978. Managing for Responsive Research and Development. San Francisco: W. H. Freeman and Company.

Blalock, A. B., & Blalock, H. M. Jr. 1982. Introduction to Social Research, second edition. Englewood Cliffs, NJ: Prentice-Hall.

Booch, G. 1986. Object-oriented development. IEEE Transactions on Software Engineering, SE-12.2, 211-221.

Clark, J. & Causer, G. 1991. Research strategies and decisions In Allan and Skinner (Eds.) Handbook for research students in the social sciences, The falmer Press, London, 163-176.

Corbin, J. & Strauss, A. 1998. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (2rd edition). (pp. 12-13). London: Sage Publications.

Cosmos Corporation. 1983. Case studies and organization innovation: Strengthening the connection. Bethesda, MD: Author.

Curtis, B. (ed.) 1985. Tutorial: Human Factors in Software Development. Los Alamitos, CA: IEEE Computer Society Press.

Davenport, T.H. & Short, J.E. 1990. The new industrial engineering: information technology and business process redesign.

Denning, P. J., et al. 1989. Computing as a discipline. Communications of the ACM, 32, 3, 9-23.

Dijkstra, E. 1968. Go to statements considered harmful. Co/7unumci3//on5o/Me ACM, 11,3, 147-148.

Faust, D., 1982. A needed component in prescription for science: Empirical knowledge of human cognitive limitations. Knowledge: Creation, Diffusion, Utilization, 3, 555-570.

Ghauri, P. & Grønhaug, K. 2005. Research Methods in Business Studies: a practical guide. 3rd edition, p. 108-109. Harlow. Pearson Education.

Guba, E. & Lincoln, Y. S. 1994. Competing paradigms in qualitative research. In N. K. Denzin & Y. S. Lincoln (Eds.). *Handbook of qualitative research*. (pp. 117- 295). Thousand Oaks: Sage Publications.

Halstead, M. H. 1977. Elements of Software Science. Amsterdam: Elsevier North-Holland.

Hedrick, T., Bickman, L. & Rog, D.J. 1993. Applied research design. Newbury Park, CA: Sage.

Hevner, A. R. & Chatterjee, S. 2010. Design Research in Information Systems: Theory and Practice. New York: Springer.

Hevner, A.R., March, S. T., Park, J., & Ram, S. 2004. Design science in information systems research. MIS Quarterly Vol. 28 No. 1, 75 - 105.

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön metodeista. [Uud. p.]. edn. Tampere: Opinpajan kirja.

Kidder, L., & Judd, C. M. 1986. Research methods in social relations (5th ed.). New York: Holt, Rinehart & Winston.

Laine, M., Bamberg, J. & Jokinen, P. 2007. Tapaustutkimuksen taito. Helsinki: Gaudeamus.

Lau, F. A. 1997. Review of action research in information systems studies. In Information Systems and Qualitative Research, A. Lee, J. Liebenau, and J.DeGross, Eds. Chapman & Hall, London, U.K., 1997, pp. 31–68.

Ledgard, H. 1987. Software Engineering Concepts. Reading, MA: Addison-Wesley Publishing Co., 111-127.

Miles, M. B., Huberman, A. M. 1994. Qualitative data analysis: an expanded sourcebook. 2nd edition. Thousand Oaks: Sage.

Mahmood, M. A. 1987. System development methods-a comparative investigation. MIS guartcWy, 11,3, 293-311.

Nunamaker, J., Minder, C. & Purdin, T. 1991. Systems Development in Information Systems

Research. Journal of Management Information Systems, 7 (3), 89–106.

Orlikowski. W. J. 1988. CASE tools and the IS workplace: Tmdings from empirical research. Proceedings of the 1988 ACM SIGCPR Conference, 88-97.

Pall, G.A. 1987. Quality Press Management. Prentice Hall, Englewood Cliffs, New Jersey.

Patton, M. Q. 1990. Qualitative evaluation & research methods. (pp.434-435). Newbury Park, CA: Sage.

Patton, M. Q. 2002. Qualitative research & evaluation methods. (3rd edition). (p.4). Thousand Oaks, CA : Sage.

Philliber, S. G., Schwab, M. R., & Samsloss, G. 1980. Social research: Gides to a decision-making process. Itasca, IL: Peacock Publishers, Inc.

Rao. H. R, Gupta. M., & Upadhyaya. S.J. 2007. Managing Information Assurance in Financial Services. IGI Global, Citation.

Robson, C. 2001. Käytännön arvioinnin perusteet. Opas evaluaation tekijöille ja tilaajille. Suom. Lindqvist, T. ym. Helsinki: Kustannusosakeyhtiö Tammi.

Sandhu, R., Ferraiolo, D., & Kuhn, R. 2000. The NIST Model for Role-based Access Control: Towards a Unified Standard." presented at 5th ACM RBAC, Berlin, Germany.

Schaad, A., Moffett, J., & Jakob, J. 2001. The Role-Based Access Control System of a European Bank: A case Study and Descussion. SACMAT 2001: 6th ACM Symposium on Access Control Models and Technologies, Chantilly, VA, USA, ACM.

Scholtz, B., Cilliers, C., & Calitz, A. 2010. Qualitative techniques for evaluating enterprise resource planning (ERP) user interfaces. SAICSIT '10: Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists. ACM. Pages 284-293.

Scott Morton, M. S. 1984. The state of art of research. In The Information Systems Research Challenge, F. W. McFarlan, ed. Cambridge, MA: Harvard Business School Press,13-41.

Simon, H. 1996. The Sciences of the Artificial. Cambridge: MIT Press.

Strauss, A. L. 1987. Qualitative analysis for social scientists. Cambridg, UK: Cambridge Universty Press.

Syrjälä, L., Syrjäläinen, E., Ahonen, S. & Saari, S. 1994. Laadullisen tutkimuksen työtapoja. Helsinki: Kirjayhtymä.

Tesch, R. 1990. Qualitative research: Analysis types and software tools. New York: Flamer.

Thomas, G. 2011. How to do your case study : A Guide for students & researchers. Thousand Oaks, CA: Sage Publications.

U.S. Government Accountability Office, Programe Evaluation and Methodology Division. 1990. Case study evaluations. Washington, DC: Government Printing Office.

Van Aken, J. E. 2004. Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules. Journal of Management Studies, 41(2), 219–246.

Yin, R.K. 2003. Applications of case study research. 2nd ed. edn. Thousand Oaks: SAGE.

Yin, R.K. 2009. Case study research : design and methods. 4th ed. edn. Los Angeles, Calif: Sage Publications.

Sähköiset lähteet.

Compliance Tutorial. 2008. How to build segregation of duties. Viitattu 18.9.2012. http://www.compliancetutorial.com/i/segregation_of_duties_ERP_security_tutorial3934.htm

Deloitte,. 2007. Segregation of Duties Solutions- Point of View, 2007. Viitattu 28.7.2012. http://www.isacahi.org/downloads/Deloitte_SOD.pdf

Henkilötietolaki. 1999. L22.4.1999/523. Finlex- Valtion säädöstietopankki. Viitattu 12.9.2012. http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Jackson, G. 2007. Identity and Access Management. Viitattu 28.8.2012. http://www.internet2.edu/pubs/200703-IS-MW.pdf

JHS 173. 2012. ICT-palvelujen kehittäminen Vaatimusmäärittely. Viitattu 10.7.2012 http://www.jhs-suositukset.fi/web/guest/jhs/recommendations/173

Jutras, C.M. 2004. Can ERP meet your technology needs? http://www.technologyevaluation.com/research/ERP

Kasanen. H. 2010. Keskitetty identiteettihallinta referenssiarkkitehtuuri. Viitattu 19.5.2012. http://www.secproof.com/media/Documents/Secproof_IdM_Referenssiarkkitehtuuri.pdf

Khan, R. 2010. Practical Approaches to Organizational Information Security Management. SANS Institute InfoSec Reading Room. Viitattu 23.7.2012. http://www.sans.org/reading_room/whitepapers/leadership/practical-approaches-organizational-information-security-management_33568

Laki väestörekisterikeskuksen varmennepalveluista. 2009. L 21.8.2009/661. http://www.finlex.fi/fi/laki/ajantasa/2009/20090661

LINARES, M. 2005. Identity Access Management solution. SANS Institute Reading Room site. Viitattu 15.6.2012. http://www.sans.org/reading_room/whitepapers/services/identity-access-management-solution_1640

Maistrati. Turvakielto. Viitattu 3.12.2012. http://www.maistraatti.fi/fi/Palvelut/kotikunta_ja_vaestotiedot/Turvakielto.

Pen State Universty. 2008; Identity and Access Management Final Report; Viitattu 21.11.2012. http://oit.ncsu.edu/sites/oit.ncsu.edu/files/roles/iam%20role/Penn_State_IAM_Final_Report.pdf

Pulman, N. & Streff, K. 2008. Identity and Access Management. IGI Publishing; Viitattu 20.11.2012. http://www.igi-global.com/viewtitlesample.aspx?id=25844

Rai, S., LLP, Y., LLP, G.R., Bresz, F., Renshaw, T., Rozek J.,& White, T. 2007. Identity and Access Management. GTAG, Global Technology Audit Guide. Viitattu 12.9.2012. http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/DownloadableDocuments/GTAG9IdentAccessMgmt.pdf

Shuey, J. & Weidner, R. 2008. Identity & Access Management Initiative. Penn State IAM Initiative. Viitattu 18.7.2012. http://its.psu.edu/IAM/

Spafford, G. 2006. Segregate Duties to Lessen Security Risks. Datamation. viitattu 9.7.2012. http://itmanagement.earthweb.com/columns/article.php/3578216/Segregate-Duties-to-Lessen-Security-Risks.htm,
http://www.datamation.com/columns/article.php/3578216/Segregate-Duties-to-Lessen-Security-Risks.htm

Tirronen. H. 2003. Tietoturvan osa-alueet käyttöturvallisuus. Viitattu 18.6.2012. http://elearn.ncp.fi/materiaali/uimonenj/VirtAMK/tturva2.html

Trochim. W., Donnelly J. P. 2007, The research Methods Knowledge. 3rd edition. SUNY-Buffalo. Viitattu 28.10.2012. http://www.socialresearchmethods.net/kb/concval.php

VM Valtiovarainministeriö. 2006A. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. Helsinki: Valtiovarainministeriö. Viitattu 28.7.2012. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061122Kaeyttoe/vahti_9_06.pdf

VM Valtiovarainministeriö. 2006 B. Tietoturvallisuuden osa-alueiden arvioinnissa käytettäviä kysymykset. Viitattu 14.7.2012. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/ILiite_6_Kaeyttoeturvallisuus.rtf

VM Valtiovarainministeriö. 2009. Lokiohje, Vahti 3/2009. Viitattu 15.8.2012. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090511Lokioh/Vahti_3_NETTI.pdf

Kuvat.

Liitteet

Tutkimuksessa käytettyt kategoriat ja datamäärien yhteenveto

Liitteet	Tutkimusdatan kategoriat ja data	Datamäärät
Liite 1	Esimiehelle lähetyt tutkimuskysymykset	27 kysymystä
Liite 2	Pääkäyttäjien haastattelu kysymykset	15 kysymystä
Liite 3	Käyttäjätunnuksien luontimäärä 01/2011 –09/2012 toimialoittain	9 toimiala (6 sivua)
Liite 4	Käyttäjätunnuksien poistomäärä 01/2011 – 09/2012 toimialoittain	9 toimiala (6 sivua)
Liite 5	Sisäisen tarkastuksen raportti + sen käyttölupa	5 + 1 sivua
Liite 6	Sosiaali- ja terveystoimialan järjestelmäpääkäyttäjän haastattelu litterointi	3 sivua
Liite 7	Sivistystoimialan järjestelmäpääkäyttäjän haastattelu 17.8.2012 klo 9:24 – 9:40 Haastattelu litterointi	4 sivua
Liite 8	Keskushallinto toimialan järjestelmäpääkäyttäjän haastattelu litterointi 20.8.2012 klo: 8:30 – 9:15	5 sivua
Liite 9	Käyttöoikeusprofiilin luomiseksi standardimalli	1 taulukko
Liite 10	Sanasto	
Liite 11	Tutkimusdatan kategoria	9 toimiala
Appendices	Publication paper	8 sivua

Liite 1.

Esimiehelle lähetyt tutkimuskysymykset

Tämä kysely on lähetetty marraskuussa 2011 ja se kuvaa sen hetkistä tialnnetta.

Kysely Vantaan kaupungin tietojärjestelmien käyttäjätunnus- ja käyttöoikeuksienhakuprosessista

Vantaan kaupungin tietohallinnon palvelukeskus on kehittämässä käyttäjähallintajärjestelmää (IDM), jonka kilpailutus on parhaillaan meneillään.

Tämän kyselyn tavoitteena on kerätä käyttökokemuksia, kehitysideoita ja parantaa nykyistä käyttäjätunnus- ja käyttöoikeushallintaprosessia, sekä erityisesti kartoittaa sitä, minkälaisia käsityksiä esimiehillä on käyttöoikeuksien hausta alaisilleen.

Keväällä 2010 sisäinen tarkastus totesi tarkastusraportissaan ”Merkittävimpien tietojärjestelmien käyttäjähallinta” muun muassa, että

- esimiehet eivät aina voi tietää, mitä ja kuinka laajoja käyttöoikeuksia eri järjestelmiin heidän alaisillaan on
- tilanteen todettiin korostuvan yksiköissä, joissa henkilöstön vaihtuvuus on suurta
- esimiehet kuitenkin päättävät ja ovat vastuussa alaistensa käyttöoikeuksista ja siksi heidän on syytä valvoa niitä säännöllisesti.

Tietohallinnon palvelukeskuksen Käyttäjähallinnan kehittämishankkeessa tavoitteena on

- kuvata käyttäjätunnushakuprosessi sekä käyttöoikeuksien merkitys ja hakukäytäntö siten, että jokainen esimies pystyy ymmärtämään, miten käyttäjätunnus haetaan mistäkin järjestelmistä, johon esimies hakee käyttöoikeuksia ja käyttäjätunnuksia.
- luoda käyttöoikeuksien hakukäytäntö, jossa esimies pystyisi yksiselitteisesti ja nykyistä helpommin arvioimaan kuinka laajaa ”vahvaa” käyttöoikeutta hän on hakemassa alaiselleen
- yhdenmukaistaa käyttäjätunnuksen hakuprosessia siten, että se soveltuu käytettäväksi kaikkien kaupungin käytössä olevien järjestelmien osalta.

Kyselyssä on kaiken kaikkiaan 31 kysymystä ja niihin vastaaminen vie noin. 15 minuuttia.

Vastaukset toivomme 4.11.2011 mennessä.

Yhteistyöterveisin,

Tietohallinnon palvelukeskus

Tewodros Guday

1. Millä Vantaan kaupungin organisaation osa-alueella työskentelet?
    - Keskushallinto
    - Maankäyttö ja Ympäristö
    - Sivistystoimi
    - Sosiaali- ja Terveystoimi
    - Tilakeskus
    - Vapaa-aika ja Asukaspalvelut
    - Keski-Uudenmaan Pelastuslaitos
    - Suun terveydenhuolto
    - Vantaan Työterveys

2. Kuinka kauan olet ollut töissä Vantaalla?
    - Alle vuoden
    - 1 – 5 vuotta
    - 6 -10 vuotta
    - 11 -15 vuotta
    - yli 15 vuotta
3. Kuinka kauan olet toiminut esimiestehtävissä?
    - Alle vuoden
    - 1 – 5 vuotta
    - 6 – 10 vuotta
    - 11 – 15 vuotta
    - yli 15 vuotta
4. Alaisten määrä
    - 1- 10
    - 11 – 20
    - 21 – 30
    - Yli 30

5. Tiedätkö millainen käyttäjätunnus- ja käyttöoikeuksienhakuprosessi Vantaalla on käytössä?
    - Kyllä
    - En
6. Tiedätkö kuka voi hakea tietojärjestelmien käyttäjätunnuksia ja käyttöoikeuksia?
    - Esimies
    - Työntekijä
    - Pääkäyttäjä
    - Tietohallinnon palvelukeskus
    - En osaa sanoa
7. Tiedätkö kuka myöntää käyttäjätunnukset ja käyttöoikeudet?
    - Oma esimies
    - Minä itse
    - Pääkäyttäjä
    - Tietohallinnon palvelukeskus
    - En osaa sanoa
8. Miten arvioit nykyistä käyttäjätunnus ja käyttöoikeuksienhakuprosessia ja siihen liittyviä toimintatapoja?
    - Käyttäjätunnus- ja käyttöoikeuksienhakuprosessi on kuvattu selkeästi
    - Prosessi ja toimintamalli tuottaa ylimääräistä työtä esimiehelle
    - Käyttäjätunnusten ja käyttöoikeuksien hakeminen kestää kauan
    - En tunne käyttöoikeuksienhakuprosessia enkä toimintatapoja

9. Oletko esittänyt käyttöoikeusmuutosta johonkin Vantaan kaupungin järjestelmään?
    - Kyllä
    - En
    - Jos kyllä, mihin järjestelmään _____

10. Miten kehittäisit käyttäjätunnus- ja käyttöoikeuksienhakuprosessia? (vapaa teksti)

11. Oletko hakenut käyttäjätunnuksia ja käyttöoikeuksia itsellesi tai alaisillesi?
    - Kyllä
    - En
12. Mihin järjestelmiin olet hakenut käyttäjätunnuksia ja käyttöoikeuksia?
    - AD- / verkkotunnus
    - Tiimiposti
    - SAP- ERP
    - SAP- SRM
    - SAP- BI
    - SAP- TRAVEL (Matkahallinta)
    - Rondo
    - GFS
    - Hijat
    - VATJ
    - WinHIT
    - Fronter
    - Efecte
    - Palvelukassa
    - En mihinkään

Muihin järjestelmiin _____

13. Tiedätkö mitkä käyttöoikeudet alaisillasi pitää olla kussakin järjestelmässä?
    - Kyllä
    - En
14. Miten saat tiedon alaisesi tarvitsemista käyttöoikeuksista?
    - Alainen selvittää itse tarvitsemansa käyttöoikeudet ja esittää minulle haettavaksi
    - Tiedän alaiseni tarvitsemat käyttöoikeudet kussakin järjestelmässä
    - Kysyn pääkäyttäjältä, mitkä käyttöoikeudet alainen tarvitsee kussakin järjestelmässä
    - Soitan Help Deskiin ja kysyn
    - Jokin muu tapa. Mikä? (vapaa teksti)

15. Oletko tarkistanut millaisia käyttäjätunnuksia ja käyttöoikeuksia alaisillasi on kussakin järjestelmässä?
    - Tarkistan ne vuosittain ja mikäli niissä on puutteita, korjaan ne/ esitän ne korjattavaksi alaiseni tehtävien mukaisiksi
    - Tarkistan ne kaksi kertaa vuodessa ja mikäli niissä on puutteita, korjaan ne asianmukaisiksi
    - En ole tarkistanut, mutta olen saanut alaisillani olevien käyttöoikeuksien listan esim. järjestelmän pääkäyttäjältä
    - En ole koskaan tarkistanut
    - En tiedä miten voin tarkistaa alaisteni käyttöoikeudet

16. Arvioitko alaisesi toimenkuvan muuttuessa hänellä olevien käyttöoikeuksien muutoksen tarpeellisuutta?
    - Kyllä, käyttöoikeudet arvioidaan ja ne pidetään ajan tasalla
    - Käyttöoikeuksiin ei kiinnitetä huomiota toimenkuvan muuttuessa
    - Muutoksen tarpeellisuus huomataan ja arvioidaan, mutta en tiedä mitä toimenpiteitä minun tulee tehdä käyttöoikeuksien ajan tasalla pitämiseksi.
17. Ilmoitatko alaisesi työtehtävien muuttuessa järjestelmien pääkäyttäjälle, että käyttöoikeudet tulee poista? (esim. työtehtävän muuttuessa tai alaisen siirtyessä Vantaan kaupungin sisällä toiseen työyksikköön ja tehtävään)
    - Henkilön työtehtävien muuttuessa ilmoitan pääkäyttäjälle roolien poistamisesta

- Henkilön työtehtävien muuttuessa ilmoitan pääkäyttäjälle, mutta en pystytä osoittamaan mitkä käyttäjäroolit hänelle on ollut käytössä
- Henkilön työtehtävien muuttuessa en ilmoita pääkäyttäjälle tilanteesta ollenkaan

18. Tunnetko käyttöoikeushakemuksia koskevat Vantaan kaupungin tietoturvaohjeet? http://intra.vantaa.fi/binary.asp?path=1;1286;5500;52437;6128;91685;6147
    - Tunnen hyvin Vantaan kaupungin tietoturvaohjeet ja noudatan niitä
    - En tiedä ohjeiden olemassaolosta
19. Joudun usein pyytämään apua käyttöoikeuksien sisältöön ja laajuuteen liittyen
    - Olen sama mieltä
    - Olen eri mieltä
    - En osaa sanoa
20. Olen saanut apua käyttöoikeuksien hakemiseen ja sisältöön liittyen (voit valita useamman kuin yhden kohdan)
    - Help Deskistä
    - Pääkäyttäjältä tai tukihenkilöltä
    - Tietohallinnon SAP- ja käyttäjähallintatiimiltä
    - Tietohallinnon palvelukeskuksen työntekijältä
    - Kollegalta
    - Alaiselta
    - VanVan tukipuhelimesta
    - Jostain muualta, mistä? _____
21. Mitä tietoja tarvitset, jotta pystyt hakemaan käyttöoikeuksia alaisillesi? (avain kenttä)
22. Millä tavalla haet käyttöoikeuksia? (voit valita useamman kuin yhden kohdan)
    - Paperilomakkeella
    - Sähköisellä lomakkeella (Efecte self- service portaalin)
    - Sähköpostilla
    - Pdf- lomakkeella
    - Puhelimella tai kysymällä joita kulta apua
23. Kaikkiin järjestelmiin, joihin haen käyttöoikeuksia, on olemassa käyttöoikeuksien hakulomake
    - Olen sama mieltä
    - Olen eri mieltä
    - En osaa sanoa
    - Jos ei, niin mihin järjestelmän _____
24. Löydätkö tarvitsemasi käyttöoikeushakulomakkeen helposti?
    - Olen samaa mieltä
    - Olen eri mieltä
    - En osan sanoa
25. Mitä seuraavista käyttöoikeushakulomakkeista olet käyttänyt? (voit valita useamman kuin yhden kohdan)?
    - Efecte - Rondo-käyttäjät
    - Efecte- SAP- loppukäyttäjät
    - Efecte- SAP-pääkäyttäjät
    - Efecte Fronter tunnuksen pyyntö
    - Efecte- Vantaan ulkopuoliset henkilöt, joita ei kirjata Hijat- järjestelmään
    - Sosiaali- ja terveysvirasto ATK-TIETOJÄRJESTELMIEN KÄYTTÖOIKEUS
    - eHIJAT / eHEVY HENKILÖSTÖJÄRJESTELMIEN KÄYTTÖOIKEUSHAKEMUS

26. Käyttöoikeuslomakkeissa olevat kuvaukset käyttöoikeuksista ovat selkeitä
    - ○ Olen sama mieltä
    - ○ Olen eri mieltä
    - ○ En osaa sanoa

27. Onko alaisillesi hakemasi käyttöoikeudet kuvattu käyttöoikeushakemuslomakkeella siten, että ne vastaavat alaisillesi tarkoitettua tarvetta ja toimintavaltuuksia?
    - ○ Käyttöoikeudet ovat kuvattu selkeästi ja pystyn ymmärtämään mitkä roolit sopivat alaisilleni
    - ○ Käyttöoikeuksia ei ole kuvattu selkeästi ja enkä pysty ymmärtämään mitkä roolit sopivat alaisilleni
    - ○ Käyttöoikeudet ovat kuvattu selkeästi, mutta en tiedä mitkä roolit sopivat alaisilleni
    - ○ En tiedä, mitä rooli-käsitteellä tarkoitetaan

Kysely on päättynyt.
Kiitos vastauksestasi

Liite 2.

Pääkäyttäjille esitetyt kysymykset

1. Ymmärtävätkö esimiehet nykyisen käyttöoikeushakuprosessi ja sen sisältö?
2. Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?
3. Onko käyttöoikeuksien hallinta keskitetty?
4. Ovatko käyttöoikeuskäsitteet selvää esimiehille?
5. Onko työntekijällä rajattu pääsy vain omiin työtehtäviin liittyviin tietoihin?
6. Onko vaaralliset työyhdistelmät tunnistettu?
7. Onko olemassa sellaisia työyhdistelmiä, joissa tarvitaan kahden tai useamman henkilön hyväksyntä?
8. Huolehditaanko tietojen päivittämisestä vastuuhenkilöiden vaihtuessa?
9. Verrataanko vastuuhenkilötietoja henkilörekistereihin (vrt. käyttöoikeushallinta)?
10. Onko käyttöoikeushallinta integroitu henkilöstörekisterin kanssa?
11. Tekeekö tietojärjestelmän omistaja/ pääkäyttäjä asiallisen tarkistuksen ennen käyttöoikeuden myöntämistä (vrt. roolit)?
12. Sulkeutuvatko käyttöoikeuksiin liittyvät käyttäjätunnukset automaattisesti tietojen muuttuessa rekistereissä?
13. Kuinka usein käyttöoikeus- ja henkilörekisterien tietoja verrataan? pv, vk, ku, miten harvemmin
14. Onko rooliin liittyvät oikeudet kuvattu riittävän tarkasti (mitkä tietojärjestelmät ja mitkä tiedot niissä)?
15. Tarkistetaanko roolien ajan tasalla olo henkilön toimenkuvan muuttuessa?

Kysymykset on otettu Vmk:n suositus tietoturvallisuuden arviointiin liittyviä kysymyksistä. (VM, 2006, B)
Kiitos

Liite 3.

Käyttäjätunnuksien luontimäärä 01/2011 –09/2012 toimialoittain

Liite 4.

Käyttäjätunnuksien poistomäärä 01/2011 – 09/2012 toimialoittain

Liite 5.

Sisäisen tarkastuksen raporttin ja sen käyttölupa
LUOTTAMUKSELLINEN

Liite 6.

Sosiaali- ja terveystoimialan järjestelmäpääkäyttäjän haastattelu
7.12.2011 klo 13:30 – 14:00
Haastattelu-Soster PK-Sound clip 01.wav

LUOTTAMUKSELLINEN

Liite 7.

Sivistystoimialan järjestelmäpääkäyttäjän haastattelu
17.8.2012 klo 9:24 – 9:40
Haastattelu-Sivi PK-Sound clip 02.wav
LUOTTAMUKSELLINEN

Liite 8.

Keskushallinto toimialan järjestelmäpääkäyttäjän haastattelu
20.8.2012 klo: 8:30 – 9:15
Haastattelu-Keha PK-Sound clip 03.wav

LUOTTAMUKSELLINEN

Liite 9. Käyttöoikeusprofiilin luomiseksi standardimalli

	Rooli profiili	Kuvaus	
Yleistietoja	Roolinimi	SD- Laskuttaja	
	Järjestelmä	SAP-	
	Roolin tekninen nimi	VFIxx_PK	
	Moduuli	Myyntireskontra	
	Kuka voi anoa	Esimies	
	Kuka voi hyväksyä	Esimies ja järjestelmän pääkäyttäjä	
	Hyväksyntätaso	Yksi (vain pääkäyttäjä)	
	Roolityyppi	Haettava rooli	
	Virka-asema	Esimies, normaalityöntekijä (molemmat)	
Toiminnallinen kuvaus	Kuvaus	Tämän rooli sisältää seuraavien tehtävien hoitamiseen liittyvät oikeudet ja raportit: • asiakasrekisteritietojen luonti ja päivitys • myyntitilauksen syöttöön liittyvät toiminnot sekä raportit • myyntitilaukset Excelistä • Rooli on tarkoitettu talouskeskuksen pääkäyttäjille	
Roolin laajuus /rajaus	Roolin laajuus / rajaus	Myyntiorganisaatiot / Yritystaso: • 1000 = Organisaatiotaso • 1210 = 01X toimiala • 1211 = 02X toimiala • 1212 = 03X toimiala • 1313 = 04X toimiala • Pääkäyttäjälle (PK) Vantaa / kaikki yrityksiin (*/*) • 1000/*, 1210/*y, 1211/*, 1212/*	Kustannuspaikat: • 10 = Toimiala10 • 11 = Toimiala11 • 12 = Toimiala12 • 13 = Toimiala13 • 14 = Toimiala14 • 15 = Toimiala15 • 16 = Toimiala16 • 19 = Toimiala19
		1000/10 1000/11 1000/12 1000/13 1000/14 1000/15 1000/16 1000/19	
Mitkä toimintoja roolissa on?	Tapahtumia /toimintoja	Myyntireskontrakyselyt F.21 = Asiakkaat: avoimet erät FD03 = Näytä asiakas (ulkoinen laskenta) FD10N = Saldonäyttö - asiakkaat MM03 = Näytä nimike & V.02 = Puutteellisten tilausten luettelo VA03 = Näytä myyntitilaus VA43 = Näytä sopimus VD03 = Näytä asiakas (myynti ja jakelu) VF03 = Näytä laskutosite XD03 = Näytä asiakas (keskitetysti) ZFBL5N = Rivit - asiakkaat	Yleiset asetukset SBWP = SAP Business Workplace SSC0 = SAP-R/3-kalenteri (työntekijä) SSC1 = SAP-R/3-kalenteri (oma) SP01 = Output Controller SM37 = Overview of job selection SU53 = Evaluate Authorization Check
Tietoturva	Vaarallinen rooli yhdistelmä	VFIxx_PK = SD-Power User PK VFIxx_PK = SD- Laskutusasiantuntija PK VFIxx_M1000 = SD- Laskuttaja M1000 VFIxx_M1211 = SD- Laskuttaja M1211	
Lisätietoja	Roolista lisätietoa antaa	Omistajaorganisaatio: Talouspalvelukeskus Yhteyshenkilö: Etunimi sukunimi	Puh:839 991 S- posti: etuni-mi.sukunimi@vantaa.fi

Liite 10. Lyhenteet

Lyhenne	Selitys
Efecte- järjestelmä	Tietohallinnon toiminnanohjausjärjestelmä
HR-järjestelmä	(Engl. Human Resources) henkilöstötietojen hallintajärjestelmä.
IAM	Identity and Access Management (Identiteetti- ja käyttövaltuushallinta)
Information Systems (IS)	Mikä tahansa yhdistelmä tietotekniikkaa ja ihmisten toimintoja, jotka tukevat operaatioita, hallintaa ja päätöksentekoa.
IDM	Identity Management
Jäljittäminen	tietojärjestelmän käyttötietojen selvittäminen
User role	Järjestelmärooli ryhmä, johon liitetään käyttäjät, joka mahdollistaa tai antaa valtuudet käyttämään järjestelmän toimintoja
Business role	Työrooli: käyttäjän työtehtävien suorituksiin tarvittava käyttöoikeuksien hallintaan tarkoitettu toimintavaltuudet
SoD	(Engl. Segrigation of Duties SoD) tehtäväroolien määrittelyn periaate, jolla rajataan tietoturvan kannalta vaarallisia käyttöoikeusyhdistelmiä.
VanVan	VanVan on nimi Vantaan kaupungissa vuonna 2008 aloitettu toiminnanohjausjärjestelmähanke, jonka toimittajana on ollut Logica Suomi Oy
ICT	information and communications technology
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
VM	Valtiovarainminsteriö
JHS	Julkisen hallinnon suositus
JUHTA	Julkisen hallinnon tietohallinnon neuvottelukunta

Taulukot

Appendices

Publication P[1]

Identity and Access management process development in the city of Vantaa: Case Study

Tewodros Guday and Rauno Pirinen
Laure University of Applied Sciences, Espoo, Finland
Email: tewodros.guday@laurea.fi, rauno.pirinen@laurea.fi

Manuscript to the Creative Education
2013. Vol.*, No.*, **-**
Published Online **** 2013 in SciRes (http://www.SciRP.org/journal/ce)

Scientific Research
DOI:10.4236/ce.2013.*****

Identity and Access management process development in the city of Vantaa: Case Study

Tewodros Guday and Rauno Pirinen
Laure University of Applied Sciences, Espoo, Finland
Email: tewodros.guday@laurea.fi, rauno.pirinen@laurea.fi

Manuscript December 30, 2012

Abstract
The main task of this study is to find out the understanding of the current user management process among the superiors on the city of Vantaa. Furthermore, it is also researcher intention to survey especially what understanding the superiors have of the user management system to their subordinates. The subject matter of the work limited to the understanding of a user management system of the organization and to the security exposures caused by their lacks. The starting point for the study is the inspection performed by the internal audit inside the city of Vantaa in the spring 2011. Internal audit accomplished a user management inspection to the most significant information systems. In the inspection, result perceived that the superiors not always necessarily have information to the different systems how comprehensive user rights their subordinates have. As a result of study research, the developing project of User Management system presented as a necessary step towards to have a significantly easier to understand the content of the user role and sustainable User Management process. The study carried out as a Case Study Research Analysis and Design Science Research study methodology while developing an Information System. The Case Study research, interview, and statistics material carried out during 2011–2012. The understanding of user management process is used as a unit of analysis in the study. The research result shows that the user roles have not been described in a sufficient way to the superiors. The superiors are not able to know what the scope of the user roles is, what operations can be done with it, what and how appropriate user role is needs to have to subordinate, and who is a contact person for the individual user role. Based on the results that obtained in the research study, "user role profile" standard model presented to the organization as a development action. The standard model helps with which methods the contents of user roles could be presented in the way understandable to the superiors.
.

Keywords row, User role, IAM, IDM, Segregation Duties SoD, Information Systems

Introduction

When the information processing systems become more complex among others without the hall of their usage, availability, information security, legislation and demands and recommendations set by the authorities will bring a big challenge to the information management units of different organizations. The user management system is a critical factor which required a follow-up constant from the information management, evaluation and R&D.

The changes on the new user groups, new network services and information distribution method in the environment, the new available services and techniques like network services and cloud services, mobile technology demands to develop the user management system. At the same time those demands increases the pressure to information management in order to develop and estimate their traditional approaching of user management system.

The internal audit of Vantaa performed the inspection on spring of the year 2011 on the user management system of the most significant information processing systems. According to the report the superiors are not always familiar and understand to the user role of their subordinates what and how wide rights they have in order to take care of their duties. This situation is emphasized in the branches in which the turnover of the staff is big.

The objective of this study is to clarify how the superiors of the city of Vantaa understand the contents of a user ID and user role management process. An inquiry with the superiors of the town of Vantaa concerning the present user management and user role management process was carried out as part of the research work and three administrators were interviewed.

As a bases of the R&D result, "user role profile" have been presented to user management process.

Sections of study

The presentation of this paper is sectioned in four different logical categories in addition to the abstract and introduction part.

In Section 1 presented an overview of Identity and Access Management (IAM) and its process. This section has also 1) the relationship between IAM components and key concepts and; 2) the automated provisioning process logical flow.

In Section 2 discusses the research methods that divided as: 1) the objectives of the study that clarify why this research paper is needed; 2) about the actual case study implementation what have a research question, interview and data mining; 3) guideline how to select appropriate research

techniques for this paper; 4) research design that illustrates the research question and; 5) also presented the process of system development research process stage in order to understand information system development.

In Section 3 presented about: 1) the process of data collection; 2) Qualitative data analysis; 3) result of the study; 4) analysis of the study and outcome of R&D contribute and; 5) significant of the study.

Section 4 is the conclusion parts that have discussion and future research question.

Overview of Identity & Access management

According to GAG9 research paper, Identity and Access Management (IAM) is a process consisting of various policies, procedures, activities, and technologies that require the coordination of many groups including human resources and IT. Identity and access management components are related to one another as **Figure 1** presented. (Rai, Ernst & LLP, 2007).

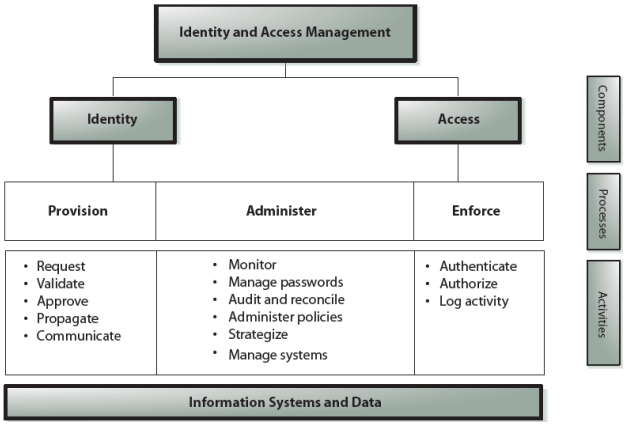


Figure 1.
Relationship between IAM components and key concepts

Identity and access management process

Understand the core concepts behind identity and access management, including single sign on, access control, authentication, authorization, identity integration, provisioning, and password management (Rao, Gupta & Upadhyaya, 2007).

According to (Rai, LLP, LLP, Bresz, Renshaw, Rozek & White, 2007), in **Figure 2** with IAM solution three important questions can be solved. a) Who has access to what information? With IAM systems, not only to manage digital identities, but also managing access to resources, applications and information these identities requite as well; b) It the access appropriate for the job being performed? The access can be examined in two ways; is the access correct and defined appropriately to support a specific job function? Does access to a particular resource conflict with other access right, thus posing a potential segregation of duties? c) Is the access and activity monitored, logged, and reported appropriately? IAM processes should be designed in a manner that supports regulatory compliance and other regulations that access rights must be defined, documented, monitored, logged, and reported appropriately.

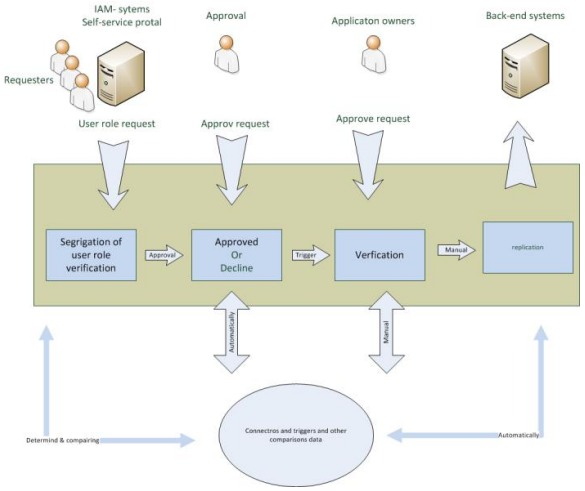


Figure 2.
Logical flow of automated provisioning process

An IAM process should be designed to initiate, modify, track, record, and terminate the specific identifiers associated with each account, whether human or nonhuman, by making use of the organization's IT resources. The organization, then, should use its IAM process to manage these identifiers and their respective association with user accounts. As a result, the IAM process should be designed to incorporate the applications a user account needs to access, and how identifiers if different between applications are associated with the user (Rai, LLP, LLP, Bresz, Renshaw, Rozek & White, 2007).

Segregations of Duties (SoD)

Dangerous work combination identifying and preventing is one of the key security mechanisms. This mechanism is called by Segregations of Duties (SoD). SoD means a situation that a person, as well as perform and approved its events or any situations in which only one or a few persons manage critical process without adequate supervision (Compliance, 2008). This kind of situation needs separation duties control. The basic objective of the separation of duties control is that anyone won't have too much power in one or more critical process (Spafford, 2006).

Designing the segregation approach rule is not an easy task, especially when an organization has vast operational information systems. It needs a good knowledge of Auditing IAM. According to (Rai et al., 2007), auditing IAM should be categorized in three topic areas: 1) Administration: What is in place to develop and maintain an appropriate IAM strategy, policies, procedures, and ongoing operations? 2) Provisioning: How is access granted, monitored, and removed within the environment? 3) Enforcement: Are appropriate measures in place to deter, prevent, and detect attempts at evading IAM processes?

According to (Rao, Gupta & Upadhyaya, 2007), presented the technologies about fraud detection knowledge and technics that called "unsupervised neural networks" which is especially used by the bank and insurance companies. In **Figure 3** presented as a summary of fraud detection tech-

niques and how they map onto different levels of fraud knowledge.

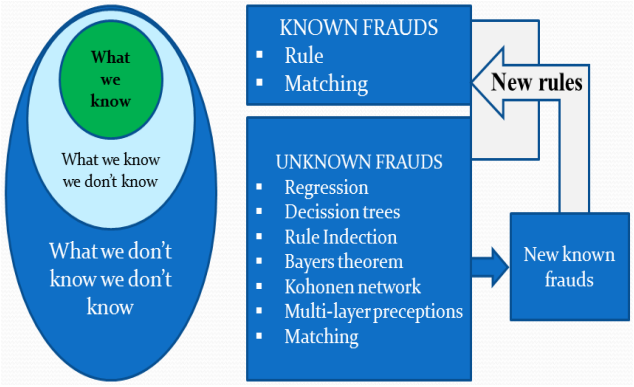


Figure 3.
Fraud detection knowledge and techniques

Research methods

This chapter discussed why the case study method used for this research and the pros and cons of the case study while in this specific research. The case study method has been used according to (Yin, 2009), presentation that is a case study of linear and iterative process, i.e.| the study plan, implementation planning, the study preparation, data collection, data analysis, and result sharing.

In addition to case study, in order to design the solution of case study result, design science research method has been studied according to the presentation of (Nunamaker, Chen & Purdin, 1991), system development research methodology. They sum up the information systems belonging to the scientific understanding of the research process, design, development, implementing production, as well as the objectives of the scheme put in place to review and assess the functioning of the system.

Objectives of Study

The proposal of internal audit by (Vantaa ICT- audit, 2011.) result draft measure has been based on systems administrator's interviews. Although the interview was made in small size and narrow scope, the proposed measurements based on the result of the interview arises some questions to the top of the issue. Why managers have a lack of knowledge of the user management process, as well as the extent of use, and how can it be improved? In order to get the answer, case study was the best solution to get the straight answers from the managers directly. On top of the case study questions, three process owners interviewed, and in order to ensure and to assess how often managers have to apply for user accounts and access rights, I made a summary of the statistical background research which carries out the numbers of the creation and deletion of user ID in the organization. Case study is of one of the comprehensive perception by examining it from multiple perspectives. Case study is characterized by an effort to find out something that is not already known and used for cases that need more in-formation is required (Yin, 2009; Thomas, 2011; Laine, Bamberg & Jokinen, 2007).

Setting of Study

This study includes the actual Case Study questions that have been grouped to four parts: the superiors' background, user management process, and the use application form of user right and the contents of user roles. The interviewees of questions are categorized according to the number of the subordinate to the branches of the organization, superior's work experience and superior. At the beginning of the inquiry, there was a covering letter which told the significance of the answers in the R&D of the inquiry target, the reasons for the inquiry, its objective. Answering the whole inquiry was voluntary and anonymous. There were 27 case study questions presented. On the basis of this case study questions, it is intended to estimate the superiors' knowledge, among others, about the user management process and about the search form and the fact whether one has been able to inform about the matter sufficiently.

In addition to the case study questions, the application owner of the three significant systems of the organization was interviewed from different branches. The application owner is responsible for the administrator of a certain system and in some cases checks in certain user roles that approved by superiors so that it is not approved too wide range of user role. Usually the superiors made contact with the application owners clarifying the contents of user rights. For these reasons, I ended up interviewing three main users.

In the application owners' interview, we went through 15 questions, and the interviews took, about 20 min. These questions are divided to two groups. Nine questions deal with the handling of the user management application process, user role to use the system maintained by the application owners. Six questions in turn deal with the main user's experience of understanding of the superior's user management process. The purpose of the application owners' interview to get the understanding is how the superiors understand the user management process in the application owners' perspective.

Guide lines how to select appropriate research technics

Case Study technic has been used for a long time in a different situation in order to contribute different kinds of solution. There are different assertions, when to use Case Study research method. (Yin, 2009) Case Study can be used in psychology (Campbell, 1975; Hersen & Barlow, 1976), Sociology (Hamel, 1992; Platt, 1992; Gerring, 2004); political science (George & Bennett, 2004), Business marketing (Benbasat, Goldstein & Mead, 1987; Bonoma, 1985; Ghauri & Gronhaug, 2002; Gibbert & Ruigrok, 2007; Graebner & Eisenhardt, 2004; Volepel, Leibold, Tekie & von Krog, 2005) education (Yin & Davis, 2006), and evaluation (U.S. Government Accountability Office, 1990).

According to (Yin, 2009), Case Study method (that I based my research) allows investigators to retain the holistic and meaningful characteristics of real-life events. So I prefer using Case Study in order to fulfil my desire to understand the challenge, why City of Vantaa user management process is not easily understandable to the superiors.

The first step was to define the "Case" being studied (Yin, 2009). In order to clarify the subject Identity and Access Management solution, challenges and consents have been covered. Then it was time to collect the relevant data and what to do with the data (Yin, 2009).

Collecting research data was a key point to the entire research. Research data that are relevant to case study can be collected (Yin, 2009) with fieldwork (Murphy, 1980; Wax, 1971), with field research (Bouchard, 1976; Schatzman & Strauss, 1973), and with social science methods more broadly (Kidder & Judd, 1986; Webb, Campbell, Schwartz, Sechrest & Grove, 1981). Collecting of data for this research is described in "setting of study part". In addition, to understand information system development and design science research, System Development Research Process has been covered that is described in the next session.

Research design

Every type of empirical research has an implicit, if not explicit, research design (Yin, 2009). So I decide to make research Case Study and planned to my research design by first setting what questions to study, what data are relevant, what data to collect, and how to analyse the result. (Phillibe, Schwab & Samsloss, 1980; Yin, 2009). It was obviously clear that (Yin, 2009) "who," "what," "where," "how," and "why" form of question provides an important clue regarding the most relevant research method to be used. Then I set to my study as a research question "How understandable is City of Vantaa's user management process to its superiors?" The understanding of user management process is used as a unit of analysis in the study. Research target is also to establish "what" is not unclear, and "what" specific challenges are in user management handling process. This result is divided by the division on the organization as the criteria for interpreting the findings (Yin, 2009) in order to address in which divisions are more challenges.

Guide lines of System Development Research Process

As (Nunamaker Jay, Chen Minder and Purdin, 1991), presented the process of System Development Research in five stages in **Figure 4**: 1) Construct a Conceptual Framework: That is consists of a) state a meaningful research questions, b) investigate the system functionalities and requirements, c) understand the system building process or procedures; d) study relevant disciplines for a new approach and ideas; (Nunamaker et al., 1991; Ackoff, Gupta & Minas, 1962; Arden, 1980; Bailey, 1982; Basili, Selby, & Hutchens, 1986; Benbasat, 1984; Blake, 1978; Blalock & Blalock, 1982); 2) Develop a System Architecture: that provides a) developing a unique architecture design for extensibility and modularity b) data functionalities of system components and interrelationship among them (Nunamaker et al., 1991); 3) Analyze & Design the System: a) that design the database or knowledge base schema and process to carry out system function and, b) Develop alternative solutions and choose one solution (Nunamaker et al., 1991; Denning, 1989); 4) Build the "Prototype" System: a) that can achieve study about the concepts, framework and design through the system building process, b) gain insight about the problems and the complexity of the system (Nunamaker et al., 1991; Scott Morton, 1984); 5) Observe & Evaluate the System: a) that the researcher observe the use of the system by case studies and field studies, b) Evaluate the system by laboratory experiment for field experiments, c) Develop new theories or models based on the observation and experimentation of the system's usage, d) Consolidate experience learned. (Nunamaker et al.,1991; Basili, 1986; Curtis, 1985; Ledgard, 1987; Mahmood, 1987; Orlikowski 1988).

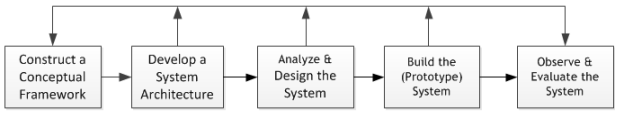


Figure 4.
A Process for Systems Development Research

Process of data collection

Using multiple source of evidence is one of a key point for this research. As mentioned earlier, the research data was collected by obtaining the research question to the superiors, by interviewing the process owners, data mining of how many incident end users has made to Service Desk in terms of user management problems, and also background research on the amount of the creation and deletion of user ID. These maintain the chain of evidence (Yin, 2009) of research data collection. The next step was how these data will be managed and analysed (Miles & Huberman, 1994), and as (Yin, 2009) mentioned "The needed analytic strategy is your guide to crafting the story". In order to managing the data to be analysed, I set four different dimensions of data categories for the research question: 1) how the security issues is taking into account; 2) Superiors level of knowledge about the user role that their subordinates have; 3) How determined the superior's on managerial responsibility on the issue of use rights and; 4) Requesting of use rights and approval process.

It also set two dimensions to the process owner interview to manage and analyse the result as follows: 1) process owners experience on how managers comprise the concepts of user role, the use of user management process, and how managers compare and keep up to date their subordinates permissions; 2) Another point of view was users and access management process and the dangerous work combinations of the system maintained by each interviewed process owners.

Qualitative data analysis

As **Figure 5** explained qualitative data analysis flow model; analysis is defined as consisting of three concurrent flow of activity: 1) data reduction; 2) data display and; conclusion drawing or verification (Miles & Huberman, 1994).

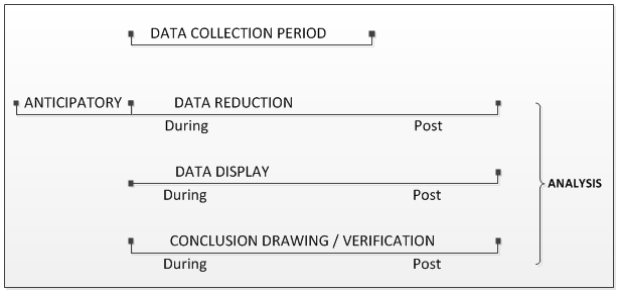


Figure 5.
Components of data analysis: flow model

Qualitative data analysis needs deep understanding (Miles & Huberman, 1994) approach of the research issue in order to interpret the phenomena well. "The use of multiple source

of evidence in case studies allows addressing a broader range of historical and behavioural issue" (Yin, 2009). However, the most important advantage is the development of converging lines of inquiry and process of triangulation (Yin, 2009; Patton, 2002).

1) Data reduction is the process of selecting, focusing, simplifying, abstracting, and transforming the data in written up field. Data reduction occurs continuously throughout the life of any qualitatively oriented project, even before the data are collected. (Tesch; 1990); 2) Data display is an organized, compressed assembly of information that permits conclusion drawing and action. In other words, it helps to understand what is happening and to do something- either analyse further to take action based on the understanding (Faust, 1982); 3) Conclusion may not appear until data collection is over, depending on the size of the corpus of field or the sophistication of the researcher, but they often have been preconfigured from the beginning. Conclusion is only half of a Gemini configuration. Conclusions are also verified as the analyst proceeds. Verification is a fleeting second thought crossing the analyst's mind during writing. The meanings emerging from that data have to be tested for their plausibility, their sturdiness, their "confirmability" that is their validity (Miles & Huberman, 1994; Strauss, 1987).

One of the essential questions of objectives of research is that: "Is the general research methods and procedures described clearly and in detail? In other word does the researcher have a complete picture, including "behind the scenes" information? Having said that this case study research expands its comprehensive collection of the relevant evidence demonstrates convincingly (Miles & Huberman, 1994; Yin, 2009).

The triangulation approach used **Figure 6** adapted from (Scholtz, Cilliers & Calitz, 2010) (in this case study: research questionnaire, process owners interview and data mining of how many incident end users has made to Service Desk in terms of user management problems, and also background research on the amount of the creation and deletion of user ID) may be the easiest to understand what makes the new socio-technical system successful (Scholtz, Cilliers & Calitz, 2010; Jutras, 2004).

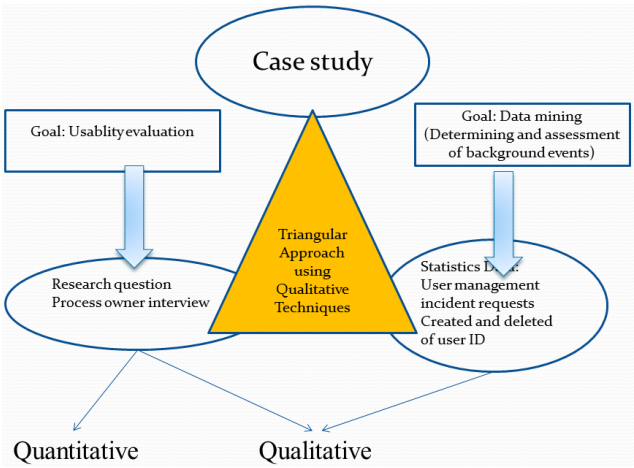


Figure 6.
Triangular Approach using Qualitative Techniques

The researcher must be able to convince the reader through the research generate findings, implications raised better (Guba & Lincoln, 1994). This study brings up the collection of data for the analysis of as a study material, that is, the understanding level of managers in user management process in different aspects.

Respondents to the research questionnaire were selected based on their position as a manager level. Almost all of the organization's managers make an employment contracts and requesting or approved user ID and permissions for different systems to their subordinates. Therefore, sending the research question to the managers was a natural choice. However, research question were sent to those who are participating in user management process frequently based on the status getting from the partially working user management system. Based on the result of the respondents, 70% managers have been more than six years of work experience in the City of Vantaa. These 70% have from six to over-fifteen years of experience as a manager level.

That means these managers have a good understanding of the organization and a strong managerial experience. Many years working in managerial positions in the organization gave them the experience and understanding of the organization information systems and user management process. Having said that, responding to the research question by that managers who earned these experiences as a manager's level and participating in user management process in a daily basis have a strong knowledge of the research question and; consequently, the result can be assumed to be reliable.

Result of the study

According to the case study research result shows that it is intended to utilize the development of an idea that is received form the case study when being developed the identity management systems of the organization. The study showed that the user role has not been described in a sufficient way to the superiors. The superiors are not able to know what are the scopes of the user roles in, functions of how the suitable user role is to their subordinates and who is the contact person of the specific user role of the system. For these reasons, the information security of the organization is vulnerable, and the user management process and handling of user role is very slow. When a job description of the subordinate's changes, the superiors are not able to know what user role on their subordinates it has been in their previous work picture.

According to the interviewed application owner's view, the superiors need clear instructions and update information about the contents of user role, what user role to use also for which task has been meant. The superiors also asked the question how long the handling of one user ID or user role takes. To solve these challenges, I design a framework model for describing of user role "user role profile" with the necessary information of user role is able to understand easily to the superior. The user role profile is a standardized model with which it is able to present the user roles of the system. The standard template makes possible the fact that the superior gets a similar view from all the user roles and is able to understand the contents and scope of any given user role. In the implementation of the future IAM project of the organization, all user roles have to be designed using user role profile template and must be described through the IAM- self-service portal to the users.

The principle of the framework of reference of the user

role profile designed by me is to clarify the contents of user role and their scope to the end users or to the superiors. The framework also give the facilitating the user role maintenance to the administrators so that the user role changing will be always made through the change management process. Furthermore, with the help of user role profile, it is able to identify in advance the segregation of user role combinations and is able to intervene and is able to control risks. With the standardization of the user role profile, the maintenance of user role is minimized, and developing them will be easy. Furthermore, the time-consuming settling disappears for the superiors' unnecessary contacts to the support service and extra time from what user role to use must be fetched to under ones it diminishes. The amount of the user support which is related to the user management also will be minimized, and at the same time the costs become smaller.

Outcome of R&D contribution

Outcome of this study is to take advantage of the organization's identity and access management in the development. The study showed that the importance of access managers may not have enough information. Supervisors are either unable to know or have time to dive in, what are their underground by the extent of use, the functionality that the appropriate license is itself subject in relation to his job function as well as who is the liaison system permissions. This is a security risk and, in addition, the user management processing is slow. When the subordinates change job position, managers are not able to know what permissions their subordinate has been in the previous duties. This make it very challenging even to compare the permission of subordinates. When the subordinates leave their duties and moved to another work unit, the process owners have a better knowledge to clear the previous permission of the subordinates. For that reason, process owners need to inform the status of the system user and permissions to the managers as regular bases. Managers needs instructions and up-to-date their knowledge of the user roles which user roles are suitable to their subordinates in order to fulfil their task.

Faced with these challenges It is designed "Role profile" model for the purpose to describe the user role, which gives the ability easily view and understand the user role scope, and other detail information to the superior. In addition, the superior's be able to justify what user roles are suitable to their subordinates while the request and approve the permission. This access profile is a standardized model which is able to present the system roles. Standard Template allows the supervisor receives a similar view of all of the roles and is able to understand the role of any of the content and scope.

When the managers requesting user ID:s and user role via self-service portal, all the related roles should be described in the user role profile model. It also designed user role profile in the form of reference to clarify the content and scope of the role to the principle of end-users or managers. It gives a framework to access to the administrator management so that editing the role is always done through a change management process. This standard model of role profile minimizes maintenance, and access to the development will become easier. In addition, with the help of user profile, it is able to identify the role of dangerous combinations predefined, and to assess and man-age the risks of dangerous combination. Supervisors' unnecessary contact with service Desk will be removed, as well as extra time-consuming is reduced. Also, the user rights associated with the use of the Service Desk amount is minimized, and at the same time costs can be reducing. Within user profile framework of my design, I took four different perspectives that support the improvement of in-formation security, as well as increase the use and handling of user management process efficiency. Points of view are described in **Table 1.**

Role Profile	
General info	Name, Name of the system, technical name, module, who can apply, who can approve, approval level, type of role
Functional description of the role	Type of duties that can perform relating to the rights and reports
The scope of the role	Organization level/ corporate level/ administrator/ cost center
What are the functions of the role?	Create, Edit, Delete etc...
Dangerous role combinations (SoD)	Role01, role02,role03
Additional info about the role	Process owner, contact person, phone, email

Table 1.
Upper level of user role profile model

Significance of the study

In this part expressed briefly summarised the study output and analysed from the prospective view of the advantage of the administration of identities and access system and risk.

It is considered as a good matter that the user management challenges have been identified by internal audit and IT-department. The IT- department has a plan, and requirements to develop the IAM- system. Furthermore, the application owners have a good knowledge of the concepts of user management process and wide expertise. However, both the case study inquiry and the interview showed that, there are weak understandings on the user roles among the superiors. Especially when the subordinates job status changes, the superiors don't' always know updating their subordinates user role as concepts of user management.

The research shows also as a second weakness that the user management process is not yet centralized and has not been concentrated for all the systems throughout the organization. On the other hand, this may not be practicable in all respects possible nor technically meaningful or cost reasons. In some systems improperly defined user rights should be developed to detecting and combating the dangerous work combinations of methods and tools. When developing IAM, the overall user management and access processes should take into account the business processes, and user management strategy premise. If so, these challenges will be corrected. Unnecessarily wildly authorized information systems user roles are a security risk. Management's lack of commitment in user management strategy is major challenges in order carry out the strategy as an organization level. Now, identifying the problems and risks are part of the organization user management processes to develop in a new way.

Developing user management process should not be IT-driven. However, it should be considered also business processes and leads by the process owners and supported by management. Business process owners have expertise in

their service-related security and legislative requirements. Information management must do more to cooperate and explore the market of available user management systems in different solutions.

Conclusion

The objective of this research is to clarify how the superiors understand the user management process and its contents. The report was conducted with interviews with three application owners and the case study questions that were drawn up on the basis of internal audit report and the researcher's knowledge of user management process. The case study inquiry was carried out with an application called Webropol which it is able to answer in Internet explorer. The study inquiry was sent by e-mail to the superiors.

In generally, the superiors identify the main features of the user management process just only the "scratch of the surface". 80% of the respondents aware of what kind of username and user management process are in use, in the organization. Despite this, more than half responded that IT-department approved or issue user ID:s and access rights, which is not true. Among managers, it is partly wrong perception of IT- department and the roles and responsibilities of application owners.

IT- department responsibility is to respond to the ICT-service production, in cooperation with business process owners and stakeholders. Information Management is not responsible for the approval of employees user role, however, for the implementation of user management process and development of the IAM- systems. The application owners are responsible for the administrative tasks of a particular system, and they do not give assent under the manager's access rights. The supervisor is responsible for evaluating what permissions his subordinates must have in each system.

According to one application owners interviewed, because IT-department creates Active directory domain user ID, the managers assume that information department approves all information systems user roles. That is not so true in reality. Generally information department does not have any rights on business process owners systems and the user management or access to systems.

Throughout the organization, managers decide for granting user role to their subordinates. In some cases, the system administrator or application owner checks the user role requests approved by the supervisor so that supervisors do not approve too broad access. In order to determine the contents of user role, managers are usually in connection with the administrator or application owners, helpdesk or are asked assistance their legality. In addition, most of the respondents were of the opinion that the user management process produced extra work.

On this basis and managers of other duties that caused rush and workloads; therefore, managers are not likely go through enough into their subordinates requested user roles content, the extent and needs of change in work duties accordance with the changes. If the wider user rights applied for the subordinate than is necessary to perform his duties or he will stay with the user roles that have been given on old tasks, then this can pose a security risk. In addition, if the segregation of duties were not taken into account while defining of the work roles description, then it may create the opportunities of emerging the dangerous work combinations and causing wide user roles may be applied for subordinates.

Further research could be how the user management process to improve the quality by using a self-service portal, as well as how improving the quality of the user management process is noticed among managers. Object of the study could be set as user management process. Another topic for further research could be risky task combinations, how to identity and access management system improve the organization's information security. The topic can be also efforts and control of dangerous work combinations.

REFERENCES

Ackoff, R. L., Gupta, S. K., & Minas, J. S. (1962). *Scientific Method*. New York: John Wiley & Sons, Inc.,

Arden, B. W. (ed.) (1980). "What can be automated?" *The Computer Science and Engineering Re-search Study (COSERS).* Cambridge, MA: MIT Press.

Bailey, K. D. (1982). *Methods of Social Research.* New York: The Free Press.

Basili, V. R., Selby, R. W., & Hutchens, D. H. (1986). Experimentation in software engineering. *IEEE Transactions on Software Engineering SE*-12, 7, 733-743.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). *The case research strategy in studies of information systems*. MIS Quarterly, 11, 369-386.

Blake, S. P. (1978). *Managing for Responsive Research and Development.* San Francisco: W. H. Freeman and Company.

Blalock, A. B., & Blalock, H. M.. Jr. (1982). *Introduction to Social Research*, second edition. Eng-lewood Cliffs, NJ: Prentice-Hall.

Bouchard, T. J., Jr. (1976). Field research methods. In M. D. Dunnette (Ed.), *Industrial and organizational psychology* (pp. 363-413). Chicago: Rand: McNally.

Campebell, D. T., (1975). *Degrees of freedom and the case study*. Comparative Political Studies, 8, 178-193.

Compliance Tutorial. (2008). *How to build segregation of duties*. Viitattu 18.9.2012. http://www.compliancetutorial.com/i/segregation_of_duties_ERP_security_tutorial3934.htm

Curtis, B. (1985). (ed.) *Tutorial: Human Factors in Software Development*. Los Alamitos, CA: IEEE Computer Society Press,

Denning, P. J., et al. (1989). *Computing as a discipline. Communications of the ACM*, 32, 3 (January 1989), 9-23.

Faust, D., (1982). A needed component in prescription for science: *Empirical knowledge of human cognitive limitations. Knowledge: Creation, Diffusion, Utilization*, 3, 555-570.

George, A.L., & Bennett, A. (2004). *Case studies and theory development in the social science*. Cambridge: MIT Press.

Gerring, J. (2004). What is a case study and what is it good for? *American Political Science Review*, 98, 341-354.

Ghauri, P., & Grønhaug, K. (2002). *Research methods in business studies: A practical guide*. Harlow, England: Pearson Education.

Gibbert, M., & Ruigrok, W. (2007). What passes as a rigorous case study? *Strategic Management Journal*.

Graebner, M.E., & Eisenhardt, K. M. (2004). The seller's side of the story: Acquisition as courtship and governance as syndicated in entrepreneurial firms. *Administrative Science Quarterly*, 49, 366-404.

Guba, E. & Lincoln, Y. S. (1994). *Competing paradigms in qualitative research*. In N. K. Denzin & Y. S. Lincoln (Eds.). Handbook of qualitative research. (pp. 117- 295). Thousand Oaks: Sage Publications.

Hamr, J. (ED.). (1992). *The case study method in socology* [Whole issue]. Current Sociology, 40.

Hersen, M., & Barlow, D. H. (1976). *Single-case experimental designs: Strategies for studying behaviour*, New York: Pergamon.

Jutras, C.M. (2004). *Can ERP meet your technology needs*? http://www.technologyevaluation.com/research/ERP

Kidder, L., & Judd, C. M. (1986). *Research methods in social relations (5th ed.)*. New York: Holt, Rinehart & Winston.

Laine, M., Bamberg, J. & Jokinen, P. *(2007) Tapaustutkimuksen taito*. Helsinki: Gaudeamus.

Ledgard, H. (1987). *Software Engineering Concepts. Reading*, MA: Addison-Wesley Publishing Co., 111-127.

Mahmood, M. A. (1987). *System development methods-a comparative investigation*. MIS guartcWy, 11,3, 293-311.

Murphy, J. T. (1980). *Getting the facts: A fieldwork guide for evaluators and policy analysts*. Santa Monica, CA: Goodyear.

Nunamaker, J., Chen, M., & Purdin, T. (1991). Systems development in information systems research. *Journal of Management Information Systems*, 7, 89–106.

Orlikowski. W. J. (1988). CASE tools and the IS workplace: findings from empirical research. *Proceedings of the 1988 ACM SIGCPR Conference*, 88-97.

Patton, M. Q. (2002). *Qualitative research & evaluation methods. (3rd edition)*. (p.4). Thousand Oaks, CA : Sage.

Philliber, S. G., Schwab, M. R., & Samsloss, G. (1980). *Social research: Gides to a decision-making process*. Itasca, IL: Peacock Publishers, Inc.

Platt, J. (1992). *"Case study" in American methodological thought. Current Sociology*, 40, 17-48.

Rao. H. R, Gupta. M., & Upadhyaya. S.J. (2007). *Managing Information Assurance in Financial Services*. IGI Global, Citation.

Schatzman, L., & Stauss, A. (1973*). Field research. Englewood Cliffs*, NJ: Prentice Hal.

Scholtz, B., Cilliers, C., & Calitz, A. (2010). Qualitative techniques for evaluating enterprise resource planning (ERP) user interfaces. *SAICSIT '10: Proceedings of the 2010 Annual Re-search Conference of the South African Institute of Computer Scientists and Information Technologists*. ACM. Pages 284-293.

Scott Morton, M. S. (1984). The state of art of research. In *The Information Systems Research Challenge*, F. W. McFarlan, ed. Cambridge, MA: Harvard Business School Press, 1984,13-41.

Spafford, G. (2006). *Segregate Duties to Lessen Security Risks. Datamation*. viitattu 9.7.2012. http://itmanagement.earthweb.com/columns/article.php/3578216/Segregate-Duties-to-Lessen-Security-Risks.htm, http://www.datamation.com/columns/article.php/3578216/Segregate-Duties-to-Lessen-Security-Risks.htm

Strauss, A. L. (1987). *Qualitative analysis for social scientists*. Cambridg, UK: Cambridge Universty Press.

Rai, S., LLP, Y., LLP, G.R., Bresz, F., Renshaw, T., Rozek J.,& White, T. 2007. Identity and Access Management. *GTAG, Global Technology Audit Guide*. Viitattu 12.9.2012. http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/DownloadableDocuments/GTAG9IdentAccessMgmt.pdf

Tesch, R. (1990). *Qualitative research: Analysis types and software tools*. New York: Flamer.

U.S. Government Accountability Office, Programe Evaluation and Methodology Division. (1990). *Case study evaluations*. Washington, DC: Government Printing Office.

Wax, R. (1971). *Doing field work*. Chicago: Universty of Chico Press.

Webb, E., Campbell, D. T., Schwartz, R. D., Sechrest, L., & Grove, J. B. (1981). *Nonreactive measures in the social science (2nd ed.)*. Boston: Houghton Mifflin.

Voelpel, S., Leibold, M., Tekie, E,, & von Krogh, G. (2005). Escaping the red queen effect in competetive strategy: Sense-testing business modles. *European Managment Journal*, 23, 37-49.

Yin, R. K., & Davis, D. (2006). State-level education reform: Putting all the pieces together. In K. Wong & S. Rutledge (Eds.), *System wide efforts to improve student achievement* (pp. 1-33). Greenwich, CT: Information Age Publishing.

Yin, R.K. (2009). *Case study research : design and methods*. 4th ed. edn. Los Angeles, Calif: Sage Publications.